Volume 7 • Issue 2 • June 2013

Editor-in-Chief
Dr. Chen-Chi Shing

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

ISSN : 1985-1553

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

VOLUME 7, ISSUE 2, 2013

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-1553

International Journal of Computer Science and Security is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCSS Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

Book: Volume 7, Issue 2, June 2013
Publishing Date: 30 - 06 - 2013
ISSN (Online): 1985 -1553

IJCSS Journal is a part of CSC Publishers
http://www.cscjournals.org

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2013

EDITORIAL PREFACE

This is Second Issue of Volume Seven of the International Journal of Computer Science and Security (IJCSS). IJCSS is an International refereed journal for publication of current research in computer science and computer security technologies. IJCSS publishes research papers dealing primarily with the technological aspects of computer science in general and computer security in particular. Publications of IJCSS are beneficial for researchers, academics, scholars, advanced students, practitioners, and those seeking an update on current experience, state of the art research theories and future prospects in relation to computer science in general but specific to computer security studies. Some important topics cover by IJCSS are databases, electronic commerce, multimedia, bioinformatics, signal processing, image processing, access control, computer security, cryptography, communications and data security, etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Started with volume 7, 2013, IJCSS appears with more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

This journal publishes new dissertations and state of the art research to target its readership that not only includes researchers, industrialists and scientist but also advanced students and practitioners. The aim of IJCSS is to publish research which is not only technically proficient, but contains innovation or information for our international readers. In order to position IJCSS as one of the top International journal in computer science and security, a group of highly valuable and senior International scholars are serving its Editorial Board who ensures that each issue must publish qualitative research articles from International research communities relevant to Computer science and security fields.

IJCSS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCSS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Computer Science and Security (IJCSS)

EDITORIAL BOARD

TABLE OF CONTENTS

Volume 7, Issue 2, June 2013

Pages

A Crypto-System with Embedded Error Control for Secure and Reliable Communication

Ranya Alawadhi *ralawadhi@smu.edu*
HACNet Labs, Bobby B. Lyle School of Engineering
Southern Methodist University
Dallas, TX, 75275, US

Suku Nair *nair@smu.edu*
HACNet Labs, Bobby B. Lyle School of Engineering
Southern Methodist University
Dallas, TX, 75275, US

Abstract

In this paper we propose a novel Crypto-System with Embedded Error Control (CSEEC). The system supports data security and reliability using forward error correction codes (FEC). Security is provided through the use of a new symmetric encryption algorithm, while reliability is provided through the support of FEC codes. The system also supports joint security and reliability in which encryption and encoding are performed in a single step. The system aims at speeding up the encryption and encoding operations and reduces the hardware dedicated to each of these operations.In addition, the proposed system allows users to achieve secure and reliable communication in which they can alternate between a priority onsecurity and reliabilityand scale their choice to the desired level in order to attain communication quality and fulfill application needs. The system targets resource constrained nodes such as remote sensor nodes operating in noisy environments.

Keywords: Joint Encryption and Error Correction, Data Security, Data Reliability, Erasure Coding, Forward Error Correction.

1. INTRODUCTION

Data security and reliability are integral aspects of modern communication systems. They are achieved through encryption and forward error correction (FEC). Conventional encryption schemes provide a high level of protection at the expense of processing time and energy. These methods force devices with constrained resources to settle for either low or no strength schemes.

Security and reliability operations have always been dealt with separately due to their contradicting objectives. There have been some efforts to combine them by joining encryption and coding into a single step. The aim was to have a faster more efficient communication in terms of time, energy, and area[1]. However, many efforts [2]–[5]did not get a lot of attention due to their large key size, high overhead or inefficient correction capability, while others[2], [4], [6]–[8]did not achieve enough strength to compete with conventional encryption schemes.

With consideration to the work that has been done previously in the area of joint security and reliability, we propose a novel Crypto-System with Embedded Error Control (CSEEC) for secure and reliable communication. Thissystem supports data security and reliability. In addition to the support of these functions separately, the systemalso supports the joint functionality when encryption and encoding are combined in a single process. CSEEC provides all these functionsusing forward error correction (FEC) codes. FEC codes are commonly used to achieve data reliability. However in this system, they are combined with specially designed operations thatallow them achieve data security as well.

To achieve data security we propose a new symmetric encryption scheme with a 128-bit key. The idea is based on the ability of erasure codes to recover from errors only when the exact locations of these errors are determined. Thus to encrypt a block of data, it is first encoded using the FEC code, then an amount equal to the amount of added redundancy is intentionally deleted. The deletion process is controlled by the encryption key. Thus, only those who possess the key are able to recover the original data. However, the idea of deletion by itself is not enough to achieve confusion and diffusion, the two properties that characterize a secure system[9]. Hence the deletion operation is combined with other operations,as well as permutation and randomization. Permutation rearranges the bits within a block while mixing combines the processed data with a random sequence. The proposed encryption scheme is not a strict block encryption sinceit does not have a traditional S-box. It is not a strict stream encryption either sinceit processes the stream of bits in fixed-sized blocks.

The support of data reliability or error control capability intuitively comes from the support of forward error correction code. This capability can be used to detect errors, correct errors, or correct erasures. The exact function will be determined by the application, the channel, and the amount of redundancy added. To achieve joint security and reliability, we extend the encryption scheme by making the amount of redundancy deleted less than the amount of redundancy added. Thus, the extra amount can be used to control the errors introduced by the channel. Due to our ability to range the amount of data deleted, the security and reliability levels are easily scaled.

CSEEC is different from previous proposals [3], [4], [11]. It does not incur any communication overhead when FEC codes are used as a mean of security. This is due to the notion of erasures, as opposite to errors. Erasure allows CSEEC to maintain the ciphertext size equal to the plaintext size. It also uses dynamic random permutations in which each processed block is permuted differently. In addition, it has a reasonable key size(128-bit)from whichall components are initialized or derived.

The rest of the paper is organized as follows. In Section 2 we discuss related work. In Section3 we describe the proposed encryption scheme. In Section 4 we present the joint reliability and security scheme. In Section 5 we provide an analysis of results showing the superiority of our method. And finally, in Section 6, we conclude the paper and describe directions for future work.

2. RELATED WORK

The first effort in the field of joint encryption and error correction was contributed by McElience[2]. McEliece introduced a public key cryptosystem based on algebraic coding theory. His idea was based on the fact that the decoding problem for an arbitrary linear code is NP-complete. The system was based on a class of error correcting code known as the Goppa code. The McEliece system is inefficient in terms of error correction capability because it requires very large public keys and large block sizes to correct the large number of errors,which result in high computational overhead. Also, the original system has been shown to be vulnerable to chosen-ciphertext attacks [12]. More work, with mixed results,have been done to extend theMcEliece system. However, the large key size remains an unsolved problem for McEliece-based systems.

A general encryption scheme based on MDS codes was proposed by Xu[13]. Xu proposed combining cryptographically strong random key stream generators with erasure correction codes. In general, the scheme makes use of any (n,k)MDS code, where $n \gg k$. A ciphertext corresponding to k symbols plaintext is chosen to be k symbols selected from the n symbols codeword generated from encoding the plaintext. The symbols are selected based on a sequence generated from the random number generator each time a plaintext block is to be encrypted. Clearly, as in stream ciphers, the security of the scheme depends on the strength of the random number generator. Further analysis is required to assess the system.

Another scheme that makes use of erasure codes was proposed in [4], a secure erasure coding scheme(SEC) for peer-to-peer storage systems. The scheme aims at ensuring the confidentiality of long term archive data through the use of the proposed encryption scheme along with fragment naming and placement procedures. SEC uses a customized version of the Reed-Solomon erasure code in whicha secret generator matrix is constructed from a user specified key by customizing the Cauchy matrix. The encryption scheme is susceptible to known plaintext attack when used in stand-alone mode.

In [3], a symmetric encryption scheme based on erasure correction codes is presented. The scheme starts by compressing and permuting the plaintext. Then, the result was encoded using an erasure correction code. The encoding phase was followed by intentional data loss through which a number of columns were removed from the block. Finally, another transposition was applied. This scheme, however, suffers from a couple of problems. The first one is the use of compression. Although compression removes redundancy, it does not add randomness [14]. In addition, compression may increase the data size when encrypting previouslycompressed data. The second issue is the key that includes all encryption parameters. This results in a large and variable key size.

An error correction cipher calleda High Diffusion (HD) cipher is presented in[5]. They used the Advanced Encryption Standard (AES) structure and replaced its diffusion layer with an error correcting code. They proposed usingHD codes that possess maximum diffusion and achieve optimal error correction. The cipher is composed of multiple iterations of the round function and key mixing operations. Though the system provides both data security and reliability, it is highly complex.

A more recent work is presented in [11], Error Correction-Based Cipher (ECBC). It is a scheme that combines error correction and security. ECBC is hardware based and designed for wireless networks. It is based on the McEliece scheme and employs a block chaining technique. The ciphertext is generated by adding a randomly generated error vector to a permuted block where the permuted block is the result of multiplying a nonlinearly transformed encoded plaintext viaa permutation matrix. In [15], it was found that ECBC is vulnerable to chosen plaintext attacks.

3. THE ENCRYPTION SCHEME

We propose symmetric encryption with a 128-bit key. The idea is to make use of the fact that a plaintext block can be recovered from a subset of the encoded block provided that enough information is available. Based on that, we intentionally introduce erasures by deleting part of the encoded block in the encryption process and later use the decoding algorithm to recoverthe deleted values from those erasures. The success of the decryption process depends on the knowledge of how erasures are introduced in the first place. Thus to prevent anyone from decrypting the data, erasures are introduced in a way known only to communicating parties.

3.1. System Parameters

Before processing the data, the sender and receiver must agree on a number of parameters. The parameters are: the error correction code $\mathbb{C}$, block size determined by the number of rows r and columns c, number of parity columns P, number of parity columns used toward reliability R, and a pseudo random number generator PRNG.

$\mathbb{C}$can be any correction code with erasure correction capability. The erasure correction codes can correct any number of erasures up to the number of added redundancy. Usually, the error correction code supports specific block sizes. Therefore, the sender and receiver must choose a suitable block size and, accordingly, determine $r$and c. For example, in Linear codes for Erasure error Correction (LEC) [16],c has to be prime and r is set at$c-1$. The selected size will depend on the application and the supported hardware capabilities and it should be chosen for fast decoding and high throughput.

Prepresents the number of extra columns that will be generated by the error correction code. Out of these Pcolumns, R columns will be used toward reliability. Thus, $P-R$ columns will be intentionally discarded and will not be included in the output. When the system is used for encryption only, R is set to zero. This means that an amount equal to the amount of added redundancywill be deletedfrom the encoded block. However, what is deleted does not necessary have to be part of the original block; it could be part of the added redundancy. This is determined by the key.

PRNG is used to generate a random sequence that is added to the processed block. This component is used to achieve the desired confusion. The selected generator will be initialized with a secret key and an initialization vector (IV). Overall, the generator should be selected with speed, efficiency, and security in mind.

3.2. Initialization

The initialization process is the same for encryption and decryption. In this process, the system state is determined and the necessary components are initialized with the shared secret key. The two main components are PRNG and a number of random permutation arrays.

The PRNGisused to generate random sequences $rSeq_i$ that will be mixed with the encoded block. The initialization process is dependent on the generator in use. Generally, this process ismade sensitive to key changes such that small changes in the key will be reflected in the generator output. It is also necessary to use a different initialization vector (IV) every time the PRNG is initialized. This is a measure taken to make sure that no relationships can be deduced from ciphertexts encrypted with same key at different sessions.

The random permutation arrays have two purposes. They are used to shuffle or arrange bits within a block and identify the columns that will be deleted from the encoded block. For these purposes three random permutations are required:

1. $P1$: is a bit permutation that will enable permuting bits within a block of size$r \times c$.
2. $P2$: is another bit permutation that will enable permuting bits within a block of size$r \times (c + R)$.
3. $P3$: is a column permutation that will specify the order of$c + P$ columns within a block.

We propose using a modified version ofthe RC4 key scheduling algorithm to derive these permutations. We are not restricted to this specific algorithm; any other algorithm maybe used as

```
procedure permutations-initialization(key,KeyLen,c,r,P,R)
   forifrom 0 to (r*c)-1
      P1[i] ←i
   enfor
   forifrom 0 to (r*(c+R))-1
      P2[i] ←i
   enfor
   forifrom 0 to c+P-1
      P3 [i] ←i
   enfor
   j ← 0
   forifrom 0 to (r*(c+R))-1
     j ←(j+Key[i mod KeyLen]+P1[i mod(r*c)])mod (r*c)
     SWAP(P1[imod (r*c)], P1[j])
     j ←(j+Key[i mod KeyLen]+P2[i])
     SWAP(P2[i] , P2[j])
     j ←(j+Key[i mod KeyLen]+P3[i mod c+P])modc+P
     SWAP(P3[imodc+P], P3 [j])
   enfor
   return (P1,P2,P3)
```

FIGURE 1: Permutation Generation Pseudo Code.

long as it can achieve the desired results and it is sensitive to small changes in the key. In other words, two keys that differ in a very small number of bits will produce two completely different sets of random permutation arrays. Furthermore, the algorithm must not be known to have any structural weaknesses that could be used later to attack the system.

To generate these arrays, we start by filling each one of them with the identity permutation and then permute them according to a key in the same way RC4 uses its key to setup its internal state. Specifically, weuse two indices and loop over all positionsand, at each iteration, swap the contents pointed by these two indices. One of these indices is incremented as a counter, while the other is incrementedrandomly using the key. To generate multiple permutation arrays, we chain them together instead of generating each one independently from the other as describe in Figure 1.

3.3. Encryption

As mentioned earlier the main idea of encryption is the partial deletion of the encoded block. However, the deletion by itself is not enough to achieve the two properties identified by Shannon [9]: diffusion and confusion. For that purpose we use dynamic permutations combined with randomization. The encryption process is described in Figure 2.

To encrypt, start by permuting the bits of the input block B_i using the permutation array $P1$. Figure 3 illustrates how a permutation array is applied to a small input block of size 3×3.

$$S_i = B_i P1_i$$

Then, encode the permuted block S_i using the agreed on $\mathbb{C}$. The encoding process will generate P parity columns, thus extending the size of the output block $T_i$to$r \times (c + P)$:

$$T_i = \mathbb{C}(S_i)$$

Next, the encoded block T_i is randomized by XORing it with the random sequence $rSeq_i$ from PRNG. The block in this step is processed row by row to make the maximum continuous sequence available from the PRNG after deletion is no more than $c - P$ bits.

$$U_i = T_i \oplus rSeq_i$$

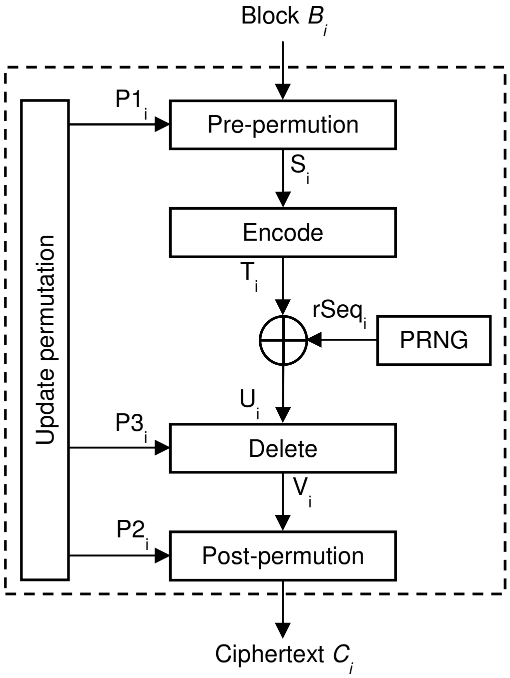


FIGURE 2: Encryption.

Data Block
D

D0	D3	D6
D1	D4	D7
D2	D5	D8

Permutation Array
M

5	7	2
1	8	0
6	4	3

Permuted Block
D`

D5	D7	D2
D1	D8	D0
D6	D4	D3

*D'= D M**

$$[D0\ D1\ D2\ D3\ D4\ D5\ D6\ D7\ D8\ ] \begin{bmatrix} 0&0&0&0&0&0&0&1&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0&0&0 \\ 1&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \end{bmatrix}$$

$$= \ [D5\ D1\ D6\ D7\ D8\ D4\ D2\ D0\ D3]$$

FIGURE 3: Permutation Example.

This is followed by the delete step where$P$ out of the $c+P$ columns are selected and removed from the randomized block. The selection is determined using $P3$. The first P entries of $P3$specify the ids of the columns that will be removed. Figure 4 illustrates this step. It shows the deletion of two columns from a 3×4data block using a permutation array.

$$V_i = U_i P3_i$$

The objective of performing the XOR operation after encoding and before deletion is to increase the complexity of the PRNG cryptanalysis. In this case, part of the generator output will be deleted and there is no way to recover what is deleted especially when is not protected by the correction code. Thus, an attacker will not have a continuous output sequence from the PRNG. Therefore, he will not have reliable knowledge as a basis for his cryptanalysis.

Data Block
D

D0	D3	D6	D9
D1	D4	D7	D10
D2	D5	D8	D11

Column Permutation
M

$$\underbrace{\boxed{\mathbf{3}}\ \boxed{\mathbf{1}}}_{\text{2 columns to delete}}\ \boxed{0}\ \boxed{2}$$

Block After Deletion
D`

D0	D6
D1	D7
D2	D8

*D`= D M**

$$= [D0\ D1\ D2\ D3\ D4\ D5\ D6\ D7\ D8\ D9\ D10\ D11] \begin{bmatrix} 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 \end{bmatrix}$$

$$= [D0\ D1\ D2\ D6\ D7\ D8]$$

FIGURE 4: Delete Step Illustration.

Finally, generate the ciphertextC_i by performing another bit permutation:

$$C_i = V_i P2_i$$

At the end of processing each block, a new set of permutation is generated. This new set allows different columns to be deleted as well as different bit permutations to be performed every time a block is encrypted. The new set is derived from the existing set using the encryption key. For that purpose, a slightly modified version of the permutation generation algorithm is used. In this version, start with the existing permutations and loop over the key bytes rather than the array entries. This means that, for those arrays with a number of entries more than the number of bytes in the key, common or fixed entries may be found in the initial set and the derived one. However, that should not affect the security of the system as a whole since the key and the initial and derived permutations are all kept secret. The update permutation algorithm is described in Figure 5.

```
procedure Update-Permutations(key,KeyLen,c,r,P,R,P1,P2,P3)
   j=0
   forkfrom 0 to keyLen-1
      j ← (j+Key[k]+P1[k])modc+P
      SWAP(P1[k], P1[j])
      j ← (j+Key[k]+P2[k]) mod r*(c+R)
      SWAP(P2[k] , P2[j])
      j ← (j+Key[k]+P3[kmod r])modc+P
      SWAP(P3[kmodc+P], P3 [j])
   endfor
   return(P1,P2,P3)
```

FIGURE 5: Update Permutations Pseudo Code.

3.4. Decryption

The success of the decryption is based on theability to identify the exact positions of the deleted data for the decoding algorithm. It is not necessary to decrypt previous blocks successfully. However, it is necessary to be synchronized with the encryption process to maintain the right system state in terms of the permutation arrays and the PRNG state. The decryption process is described in Figure 6.

To decrypt, start by reversing the post-permutation:

$$V_i = C_i P2_i^T$$

Then, identify deleted columns using $P3$ and rearrange them into their proper order. This step will expand the block to include the deleted columns. This is an important step for successful decryption for a number of reasons:(1) to ensure that the XORing with the random sequence is performed correctly and (2)because the order of symbols is as important as the value of symbols to decoding.

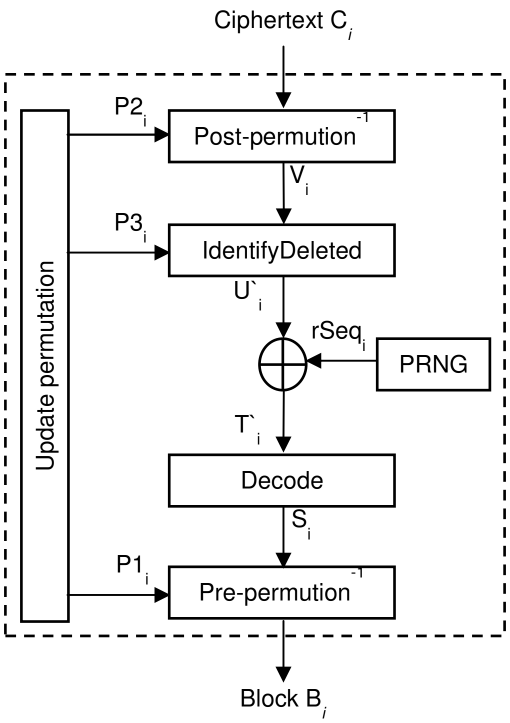
$$U_i' = V_i P3_i^T$$

Once the columns are put in order, the data can be extracted by adding $rSeq_i$:

$$T_i' = U_i' \oplus rSeq_i$$

Next, reconstruct the P deleted columns using the decoding algorithm of $\mathbb{C}$:

$$S_i = \mathbb{C}^{-1}(T_i')$$



Finally, recover the plaintextB_i by reversing the bit permutation:

$$B_i = S_i P1_i^T$$

FIGURE 6: Decryption.

As in encryption, after processing a block, a new set of permutation arrays are generated. They are derived from the existing one using the algorithm described in Figure 3. The permutation update function in decryption must be identical to the one in theencryption ifupcoming blocksare to be decrypted successfully.

4. JOINT SECURITY AND RELIABILITY

Joint securityand reliability allows us to perform encryption and error control simultaneously in a single process. This process is an extension ofencryption where the number of deleted columns is less than the number of added parity. In this scenario, when determining P one needs to consider how many columns will be deleted and how many will be added for error control purposes.

The number of deleted columns is set with the amount of securitythat is required in mind. The more columns deleted the more complex the attacks on the system get, and the more columns need to be reconstructed. Generally, the decoding process is more expensive than the encoding one,which means the more columns recovered the more delay one may expect. Overall, the number of columns deleted should not affect the system performanceand, at the same time, should achieve the desired security level.

As to those columns added for error control, one needs to determine what type of error control is required: error detection vs. error correction. This will be determined by application needs and thecommunication channel. Based on the channel, the type and number of errors expected may beidentified. Consequently, R is determined suitably. In case R is set to be equal to P, then no columns will be removed and the securityof the data will be maintained only by the randomization and permutations.

Once the system parameters are determined, the initialization process can be followed as in Section 3.2. In this process the key is used to set up the system by initializing the PRNG and deriving the random permutations. Upon successful initialization the blocks can be processed, essentially, as in the encryption case(Figure 2). First, the bits of B_i are permuted within the whole block. Then, the permuted block is encoded by $\mathbb{C}$ where P extra columns are generated. Next, the encoded block is XORedwith a random sequence generated from the PRNG. This is followed by the deletion step where the encryption and the joint functions differ. In this case, $P - R$ columns are deleted using $P3$ where the first $P - R$entries determine the ids of those columns. Finally, coded ciphertext is generated by permuting the bits within the whole block where the masked parity and data bits are mixed together. The encoded ciphertext C_i is expressed as follows:

$$C_i = \left(\mathbb{C}\left(B_i P1_i\ \right) \oplus rSeq_i\right) P3_i\ P2_i$$

Error control can only be performed by those who possess the key. To be able to at least detect channel errors, the permutation and XOR steps must be reversed first before applying the decoding process. Those two operations—although performed on data as well as parity bits—do not propagate errors when they occur.

To decrypt an encoded ciphertext C_i, proceed as in Figure 6. First, the bit permutation is reversed. Then, the deleted columns are identified and the remaining ones are rearranged in their proper order with the use of $P3$. Next, the random sequence is extracted by XORing it back with the block. The decoding algorithm is then applied to recover the deleted columns and detect or correct communication errors. Communication errors can only be handled if they are within the capability of the correction code. Finally, the bit permutation is reversed to obtain the plaintext block B_i back.

$$B_i = \ \mathbb{C}^{-1}(C_i P2_i^T P3_i^T\ \oplus rSeq_i)\ P1_i^T$$

4.1. Data Reliability

Data reliability, where no security measures are required, is achieved through the use of forward correction codes. These codes are used to detect errors, correct errors, or correct erasures. The exact functionality is determined by the application and communication channel. These two factors also determine the number of parity added to the data. In this case, R is set to be equal to $P$and only the correction code is used without the other operations.

For reliable communication, data is encoded using the agreed on error correction code. The encoding process generates P parity columns. Then, the data along with the parity are sent to the destination. At the other end, the decoding algorithm is executed to detect errors and if possible correct them, or, in case of erasures, if they are identified, they are corrected in orderto recover the original data.

5. ANALYSIS

This section provides an assessment of the proposed scheme in terms of security, randomness, and highlights the system performance. In terms of the correction capability, the analysis is the same as the analysis applied to the error correction code as no modification is applied on the code itself. However, when considering the correction capabilities of the code with respect to communication errors, one needs to consider the amount of redundancy assigned to the reliability rather than the amount of redundancy generated from the code.

5.1. Security

The security of the system depends on how hard it is to find the encryption key. CSEEC key is used in two ways: to initialize the PRNG and to derive the random permutations. Extracting the key from the random permutation is a very challenging task for a number of reasons. First, these permutations are kept secret. Second, the permutations are updated every time a block is processed, which means there will not be enough blocks that use the same permutations for analysis. Third, the randomization and deletion add an extra burden on the process of extracting the key. Thus, extracting the key from the PRNG output sequence isa more applicable approach in determiningthe key.

For known PRNGs, there are a set of attacks that can be applied to determine the key used to initialize the PRNG state. However, any attack can only be applied on reliable knowledge of the output sequence, which is not the case here. All the PRNG sequences used to encrypt any ciphertext are randomly permuted and partially deleted. Thus, before applying any attack, the effect of the random permutation and deletion need to be reversed first to be able to identify the PRNG sequence. These operations are guided by the unknown key that we want to find and the only way to reverse these operations is by trying every possibilityin which these operations can be performed.

For known plaintext attacks, the number of possible PRNG sequences used in randomizing a single block is determined by the number of possible pre-permutations, post-permutations, number of ways to select deleted columns, andthe values ofthe deleted columns. These possibilities are determined as follows:

- The number of permutations that result in unique sequences is determined by the number of ones or zeros in a sequence, and that number is maximal when the sequence is balanced. Thus, the maximum number of possible pre-permutations is $\binom{r \times c}{r \times c/2}$ and post-permutations is $\binom{r \times (c+R)}{r \times (c+R)/2}$.
- The number of possible ways to select *P-R* columns from a block with $c+P$ columns is $\binom{c+P}{P-R}$.
- The number of possible values that can be assigned to$P-R$ deleted columns is $2^{r*(P-R)}$.

Using the above possibilities brings the number of possible sequences generated from the PRNG for a single block to

$$\binom{r \times c}{r \times c/2} * \binom{c+P}{P-R} * 2^{r*(P-R)} * \binom{r \times (c+R)}{r \times (c+R)/2} \quad 1$$

Fora chosen plaintext attack, the ability to customize a plaintext can reduce the number of possible PRNG sequences. In this case, the effectof the pre-permutation can be eliminated by setting the plaintext to all zeros or all ones. Thus, the number of possible PRNG sequences is reduced to:

$$\binom{c+P}{P-R} * 2^{r*(P-R)} * \binom{r \times (c+R)}{r \times (c+R)/2} \quad 2$$

Once the possible sequences are determined, then an attack is applied on each candidate sequence until the right key is determined. However if the attack in consideration requires a long sequence of size Qthat expands multiple blocks, then the above enumeration is repeated for each block until a sequence with the desired length is obtained.This sums up the total number of possible candidates for known plaintext attacks to:

$$\left(\binom{r \times c}{r \times c/2} * \binom{c+P}{P-R} * 2^{r*(P-R)} * \binom{r \times (c+R)}{r \times (c+R)/2}\right)^{\frac{Q}{r \times (c+R)}} \quad 3$$

And for chosen plaintext attacks to:

$$\left(\binom{c+P}{P-R} * 2^{r*(P-R)} * \binom{r\times(c+R)}{r\times(c+R)/2}\right)^{\frac{Q}{r\times(c+R)}} \qquad 4$$

The above formulas are used to express how much it takes just to prepare the data before applying an attack. This is the amount by which the complexity of an attack is increased.

It is clear that the security of CSEEC depends on the security of the PRNG. The level of security also depends on the combination of parameters. This dependence allowsusing less secure more efficient PRNG without compromising the confidentiality of information. Therefore, when setting these parameters one should consider the effect of these choices on the overall security of the system and whether these choices result in reachingthe targeted security level.

If it is necessary to use the same key again, then a distinct initialization vector must be used for every PRNG initialization process. This is a necessary condition to ensure the following:

$$C_1 \oplus C_2 \neq C_1' \oplus C_2'$$

where C_1, C_2, C_1' and C_2' are the ciphertexts that correspond to the following plaintexts B_1, B_2, B_1' and B_2' respectively and the plaintexts satisfy the following:

$$B_1 \oplus B_2 = B_1' \oplus B_2'$$

5.2. Randomness

One of the criteria used to evaluate any cipher is the assessment of its suitability as a source of randomness. A good cipher is a cipher that can be considered a true random number generator. Randomness testing is used for that purpose. Such tests do not guarantee that the generator is indeed random, however, the more tests the generator passes, the more confidence they give in its randomness.

We used the National Institute of Standard and Technology (NIST) statistical test suite for random number generators [17]. The suite consists of 15 core tests that are extended to 188 tests under different parameter inputs [18].

For the purpose of evaluation, we selectedthe Reed-Solomon code with two stream ciphers as random number generators, Grain-128 [19] and A5/1. Grain-128 is a 128-bit stream cipher designed for highly restricted environments. A5/1 is a 64-bit stream cipher used in GSM communications. The key setup process for A5/1 is extended to incorporate all the 128 key bits used by CSEEC. Both of these selections have good statistical properties and are chosen for their efficient hardware evaluations.

To evaluate the system against randomness, we developed two data sets. The first data set evaluated the randomness of the ciphertexts. A sequence in this set wasthe result of concatenating ciphertexts formed from encrypting random plaintexts and one random key wasused per sequence. The second one evaluated the correlation between plaintexts and ciphertexts. Each sequence in this set consisted of blocks formed from XORing a plaintext with the corresponding ciphertext.One random key was used per sequence.

As for the system parameters, $r$was set to 8, c to 16 and P to 3. We ranged R from zero to P for each data set. A total of 16 samples were generated, each with300 sequences. Then, all the 188 tests were applied with the default parameters.

R	0	1	2	3
Ciphertext block Size	128	136	144	152
Sequence Length	1,048,576	1,048,696	1,048,608	1,048,648
Data Set 1	0/188	0/188	0/188	0/188
Data Set 2	0/188	0/188	0/188	0/188

TABLE 1: NIST Tests Result for Grain-128 and A5/1.

The results of the two generators were the same: all tests were passed. Table 1 shows the number of failed tests for each data set and the range of values for R. The results obviously depend on the randomness of the PRNG in use. As expected, the randomness of CSEEC output depends heavily on the randomness of the random number generator. However, the goal of these tests is to examine the effect of the other operations: permutations and, specifically, deletion on the output of the PRNG and whether these operations change the statistical properties of the output sequence. Asthe results indicate, the permutations and deletion do not affect the randomness of the PRNG in use.

5.3. Implementation

The scheme was implemented in software and hardware as a proof of concept. The goal of the software implementation was to verify the correctness of the algorithm and to generate the data for randomness testing. On the other hand, the goal of the hardware implementation was to understand the complexity associated with each operation.

An RTL implementation was made for the described algorithm and Altera Quartus II was used to simulate the design using a Stratix III device (EP35E50F780C2). The implementation generates 3 parity symbols using Reed-Solomon (RS) encoding for each block of size 8×8. Thus, up to 3 columns can be deleted from a block. The implementation results are shown in Table 2. The numbers in this table do not include the area dedicated to the PRNG nor the error correction code because it is assumed that a system that implements CSEEC will already have these two functions implemented. The throughput of encryption is 96 Mbps and decryption is 95 Mbps. Comparingthese numbers with other encryption schemes indicates that CSEEC has good processing speed. However, comparing the joint functionality of CSEEC with encryption schemes combined with error correction codes shows that CSEEC exceeds them since the time it takes to process a block does not change whether the scheme is used for security or for joint security and reliability. On the other hand, when any encryption scheme is combined with error correction code then the time to process a block isincreased by the amount it take to encode or decode a block.

Operation	Encryption	Decryption
Frequency	53.75 MHz	79.28 MHz
Logic Utilization	14%	21%
Combinational ALUTs	3,964	6,279

TABLE 2: Hardware Implementation Results.

6. CONCLUSION AND FUTURE WORK

A novel systemthat provides data reliability and security using FEC is proposed. The user is given the option to choose both or either services depending on his/her needs. Data security is achieved through a new encryption scheme based on intentional deletion. Joint securityand reliability is achieved through the extension of the encryption scheme by intentionally deleting an amount less than the amount of added redundancy.

The system was implemented withthe Reed-Solomon code and two possible PRNGs, Grain-128 and A5/1. The system design is general enough that it can use any forward error correction code and any PRNG. Thus, users have the ability to use existing implementations with minimum additional operations. It is shown that the system security depends on the strength of the combination of its components, not on the individual security of each one of them. Moreover, the randomness of the PRNG is preserved and reflected in the system output. Also the implementations show the applicability and superiority of the scheme.

Currently, the hardware implementation is being optimized and possible enhancements to the algorithm are being investigated. It is expected that processing speed can be further enhanced.

7. REFERENCES

[1] O. Adamo and M. R. Varanasi, “Hardware based encryption for wireless networks,” presented at the Military Communication Conference, 2010, pp. 1800–1805.

[2] R. J. McEliece, “A Public-Key Cryptosystem Based On Algebraic Coding Theory,” *Deep Space Network Progress Report*, vol. 44, pp. 114–116, Jan. 1978.

[3] S. Nair, E. Celikel, and M. Marchetti, “Adaptive Security and Reliability using Linear Erasure Correction Codes,” in *Proceedings of 7th International Business Information Management Conference*, Brescia, Italy, 2006.

[4] J. Tian, Y. Dai, and Z. Yang, “SEC: A practical secure erasure coding scheme for peer-to-peer storage system,” *14th Symposium on Storage System and Technology*, pp. 210–222, 2006.

[5] C. H. Mathur, “A Mathematical Framework for Combining Error Correction and Encryption,” Ph.D. Dissertation, Stevens Institute of Technology, Hoboken, NJ, USA, 2007.

[6] R. Ma, L. Xing, and H. E. Michel, “Fault-Intrusion Tolerant Techniques in Wireless Sensor Networks,” in *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, 2006, pp. 85 –94.

[7] W. Godoy Jr and D. Pereira Jr, “A proposal of a cryptography algorithm with techniques of error correction,” *Computer Communications*, vol. 20, no. 15, pp. 1374–1380, 1997.

[8] T. Hwang and T. R. N. Rao, “Secret error-correcting codes (SECC),” in *Proceedings on Advances in cryptology*, New York, NY, USA, 1988, pp. 540–563.

[9] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

[10] C. E. Shannon, “A mathematical theory of communication,” *Bell Systems Technical Journal*, vol. 27, pp. 379–423, 1948.

[11] O. Adamo, E. Ayeh, and M. Varanasi, “Joint encryption error correction and modulation (JEEM) scheme,” in *2012 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, 2012, pp. 1–5.

[12] T. A. Berson, “Failure of the McEliece Public-Key Cryptosystem Under Message-Resend and Related-Message Attack,” in *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, London, UK, 1997, pp. 213–220.

[13] L. Xu, “A general encryption scheme based on MDS code,” in *Information Theory, 2003. Proceedings. IEEE International Symposium on*, 2003, p. 19.

[14] W. Chang, B. Fang, X. Yun, S. Wang, and X. Yu, “Randomness Testing of Compressed Data,” *Journal of Computing*, vol. 2, no. 1, Jan. 2010.

[15] Q. Chai and G. Gong, “Differential Cryptanalysis of Two Joint Encryption and Error Correction Schemes,” in *2011 IEEE Global Telecommunications Conference (GLOBECOM 2011)*, 2011, pp. 1 –6.

[16] Z. Alkhalifa, “Application and system layer techniques for hardware fault tolerance,” Ph.D. Dissertation, Southern Methodist University, Dallas, TX, USA, 1999.

[17] “NIST.gov - Computer Security Division - Computer Security Resource Center.” [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/index.html.

[18] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Aandel, D. Banks, A. Heckert, J. Dray, and S. Vo, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” National Institute of Standards and Technology, Apr. 2010.

[19] M. Hell, T. Johansson, A. Maximov, and W. Meier, “The Grain Family of Stream Ciphers,” in *New stream cipher designs the eSTREAM finalists*, vol. 4986, Berlin; New York: Springer, 2008, pp. 179–190.

Security Aspects of the Information Centric Networks Model

Amjad Mahfouth *amahfouth99@gmail.com*
Computer Information System
Al Quds Open Univeristy
Tulkarm,00970,Palestine

Abstract

With development of internet and the enormous growth of contents over networks, that motivated the researchers to proposed new paradigm model called Information Centric Networks ICN , the most features of ICN model is based on the content itself, instead, of the server located the contents over internet. This new model has a lot of challenges such as, mobility of contents, naming, replications, cashing, communications, and the security issue to secure the contents, customer, and providers. In this paper we will focus on ICN Model and propose solutions of security to protect the network elements, since the security is based on the packet itself rather than the host-centric.

Keywords: ICN, Denial of Service, Encryption, Digital Signature.

1. INTRODUCTION

The enormous growth of information's, resources, contents over internet and networks, increased demands of the content over internet, translation of contents between different networks, and the complexity of the networks and telecommunication system, that's motivated the researchers to explore a new network paradigm called Information Centric Networks (ICNs), in order to adaptive the growth and complexity of contents' and networks over internet. The most features of Information Centric Networks are the availability and mobility a lot of services to customers and users were offered by different providers and operators. According to [1] statistics, In 2011, mobile traffic rose to 144% than previous year, the annual growth of consumer mobile traffic from 2011 to 2016 is expected 83%, while the global mobile data volume is expected to be 10.8 Exabyte per month in 2016. That's an evidence of increase demand of information from side, and growth of the risks on the contents over internet from other side. Therefore the challenges of security, mobility of contents in Information Centric Networks Models are very complex with the complexity of networks technologies. The applications and services were offered to customers have own authenticity method and use different credentials, reliable and easy-to-use methods are needed to support the new paradigm.

The rest of paper is organized as follow: in section 2, we present and discuss the problem statement of the paper, section 3, describe and present the ICN models with their research projects and its features and challenges, section 3, "security issue" in this section we will discuss and propose new security solutions to protect the contents over network. In last in section 4, we prepare the conclusion and summarize the most features and challenges of ICN model and finally we ask several question related to the security model and its features.

2. PROBLEM STATEMENT

With development of Internet, development of business work over internet and increased the web application based on internet, that's lead to customer eyes to look at internet as major of their business, socials , entertainment , news, searches and a lot of their several interests. The huge capacity of in formations, networks, Telecommunication, translation of information between customers and providers, between different networks over internet , that exerts more challenges to the existing internet architecture, especially, in the appearance of the complexity and the creativity of Next generation Networks and the appearance of Intelligent devices and Intelligent home, all of the these challenges and the future development of applications , that leads to re-think with existing architecture and explore new paradigm architecture organize the contents over internet and keep its availability for customers. Through dynamic method that achieving the efficiency of contents over internet compared with the existing internet architecture, since the users are interested with availability of contents rather than the contents where resident in networks. The new paradigm called Information Centric Network s(ICNs).

The idea behind of Information Centric Networks approach are modeled using on getting the actual contents instead of host centric architecture approach, which means, the ICN model does not focus on the location of contents, in which server located, and server hosted as the existing architecture. Many of researches projects are modeled on Information Content Networks such as: [2]-[6] most of these researches have been described the Information Centric Information from side and underlying the problems and the solutions of ICN architecture from other side, since every architecture or paradigm have a lot of challenges such as, problems, description of implementation technique on the architecture ,and its hierarchy structure. The ICN architecture is in structure and discussion stage, so a lot of proposed solutions are modeled to describe the ICN architecture with it features.

In this paper we will discuss the Information Centric Networks features, challenges, problems and the security technique on the ICN networks to protect the customers, contents and providers over internet.

3. THE INFORMATION CENTRIC NETWORK APPROACH

The increasing demand [6] for highly scalable and efficient distribution of contents over internet has motivated to develop new network called information-centric networks (ICN), which is based on named data objects.

In current architecture networks approach are host-centric which require contents locations in order to get the contents, also the network communication is based on name host, for example, web servers, PCs, laptop, handset devices and other devices. While in the ICN architecture the users get the contents regardless of the host- centric or the server located the contents, this mobility allows the users to share their contents and data anywhere and anytime. In addition the common goal of ICN in [7] is to achieve efficient and reliable distribution of contents by providing general platform for communication services that are today available in dedicated system such as peer-to-peer(p2p) overlays and proprietary content distribution networks.

The presented ICN architecture explode new challenges features based its structure and its architecture, such as supporting of mobility agent of content , cashing, replications, communications, names of data contents and security challenges of model. For each of those features, we can propose a new methodology for thesis in order to classify, checks the optimality, describe the techniques and its architectures, determine the work base, and finally the relation between others features in the network model. Since all of those features were analyzed, and proposed solutions and techniques regards with their details and point of views on project researches which proposed in [2]-[6].

In this paper we will focus on the methodology of security techniques on the model in order to protect the contents over its mobility, cashing, replications, and communications between the users and providers.

There a lot of projects were studies and proposed improved solution of ICN network such as [7]:

- TRIAD project (www-dsg.stanford.edu/triad/) [2].
- Data-Oriented Network Architecture (DONA) [3].

- Content-Centric Networking (CCN) [5], currently in the Named Data Networking (NDN) project (www.named-data.org)
- Publish-Subscribe Internet Routing Paradigm (PSIRP) [4], now in the Publish-Subscribe Internet Technology (PURSUIT) project (www.fp7-pursuit.eu)
- Network of Information (NetInf) from the Design for the Future Internet (4WARD) project [6], currently in the Scalable and Adaptive Internet Solutions (SAIL) project (www.sail-project.eu)

While of these projects approaches were different from each others with respect to their details, analysis and the techniques of routing name, cashing, request/receive and publish the contents and the its procedure algorithm, mobility and security in the ICN Models, they share many assumption, objectives and architectural specifications. The aim is to develop a network architecture that is better for efficiently accessing and distributing content and that is better cope with disconnections, disruptions effects in the communication service.

4. CONTENT SECURITY MODEL

Since the ICN approaches [8] resulted in content arriving from networks elements other than the locating server, the security model cannot be based on where the packet come from or locating server, instead, ICN design must secure the content rather than path, as suggested in [9][10] and else.

The ICN papers are promising for better security due to the use of digital signatures and securing the packet itself. To ensure the confidently, security of packet are self certifying, packet are authenticated using digital signature, also securing the communications lines between users and providers, and providing encryption/decryption in each packet to secure the packet and provide the confidently. The customers who request the resources or the contents must know the name of contents, in addition the customer must know the contents providers public key, so that he can verify the originality and integrity of content. Therefore the ICN model itself must bind the objects name with its public key of content providers'. To falsify the contents an attacker must register with the ICN system, in result, it mitigated the denial of service attack against the contents due to content-centric flow of traffic rather than the host-centric. Naming contents over ICN model explode the directions of naming object through DNS names as suggested in [11][12], the first naming uses hierarchical human-readable-names, the second naming systems uses self-certifying names, which is un readable by human, the key is bound to the name itself, so the users must use other techniques to determine the name of contents through search engine, or personal provider.

Resources which are requested using the interest packet must have permission or know the key to get validate. Therefore denial of services DoS attacks against resources and providers is mitigated due to packet flow of traffic.

5. CONCLUSION

In this paper we discussed and analyzed the ICN Model approach, also we explained the reasons that motivated the researcher to establish and create the model due to the enormous growth of contents over internet, and achieving the availability, mobility of contents and providing more security strategy to protect the contents, users and consumer of ICN model rather than host-centric. In addition we proposed the most features and challenges in ICN models likes, naming, routing, mobility, cashing and security of contents over ICN Model, and we browsing most the researches project, that studies and proposed a lot of different solutions and techniques on ICN model, regards their analysis, point of views, and their experiments techniques. Finally we proposed solution techniques on security models to protect the ICN models regards with its components like, contents, providers, operators, customers, and its features. In addition of the authenticity of contents itself, generating the public key, naming of request model, and the encryption in the content itself, and providing secure communication between source and destination.

Since the ICN model is very young and proposed solutions are insufficient and incompatible. We can ask some of questions, we can trust of security model which presented in this paper to secure the ICN model or not, also does the encryption/decryption need more complex computation, does that effect on the efficiency, availability, and traffic packet in ICN model. Is the system reliable or not. Also we can ask others questions on ICN model features about routing, cashing and naming, does they satisfy the efficiency, privacy, keep availability of system and scalability. We can answer on all of these questions in next future researches.

6. REFERENCES

[1] CiscoSystems. (2011). Cisco Report for IP Growth for 2011-2016. Internet Report, 1, 3.

[2] Cheriton, D. R., & Gritter, M. (2000). TRIAD: A new next-generation Internet architecture.Retrieved from. Available on : http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.33.5878.

[3] Koponen, T., Chawla, M., Chun, B.G., Ermolinskiy, A., Kim, K. H., Shenker, S., & Stoica, I. (2007). A data-oriented (and beyond) network architecture. SIGCOMM Comput. Commun. Rev., 37(4), 181–192. doi:10.1145/1282427.1282402.

[4] Dimitrov, V., & Koptchev, V. (2010). PSIRP project – publish-subscribe internet routing paradigm: new ideas for future internet. In Proceedings of the 11th International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing on International Conference on Computer Systems and Technologies (pp. 167–171). New York, NY, USA: ACM. doi:10.1145/1839379.1839409.

[5] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. L. (2009). Networking named content. In Proceedings of the 5th international conference on Emerging networking experiments and technologies (pp. 1–12). New York, NY, USA: ACM. doi:10.1145/1658939.1658941.

[6] B. Ahlgren et al., “Second NetInf Architecture Description,” 4WARD EU FP7 Project, Deliverable D-6.2 v2.0, Apr. 2010, FP7-ICT-2007-1-216041- 4WARD / D-6.2, http://www.4ward-project.eu/.

[7] Bengt Ahlgren, Christian Dannewitz, Claudio Imbrenda, Dirk Kutscher, and Börje Ohlman, A Survey of Information-Centric Networking. 0163-6804/12/, 2012 IEEE IEEE Communications Magazine. July 2012.

[8] Ali Ghodsi, Teemu Koponen, Barath Raghavan, Scott Shenker, Ankit Singla, Janes Wilcox, Information-Centric Networking. Seeing the Forest for the Trees, Cambridge, MA,USA. copyright 2022, ACM 978-1-4503-1059-8/11/11, 2011.

[9] M. Walfish, H. Balakrishnan, and S. Shenker. Untangling the Web from DNS. In Proc. of NSDI, 2004.

[10] D. Wendlandt, I. Avramopoulos, D. Andersen, and J. Rexford. Don’t Secure Routing Protocols, Secure Data Delivery. In Proc. of HotNets, 2006.

[11] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker. Naming in Content-Oriented Architectures. In Proc of SIGCOMM, Workshop on ICN, 2011.

[12] D. Smetters and V. Jacobson. Securing Network Content. Technical report, PARC, October 2009.

Secure Image Encryption Using Filter Bank and Addition Modulo 2^8 with Exclusive OR Combination

Saleh Saraireh *saleh_53@yahoo.com*
Department of Communications and Electronic Engineering
Philadelphia University
Amman,Jordan.

Mohammad Saraireh *srayreh_2000@yahoo.com*
Department of Computer Engineering, Mu'tah University
Karak, Jordan

Yazeed Alsbou *yazeed_alsbou@yahoo.com*
Department of Computer Engineering, Mu'tah University
Karak, Jordan

Abstract

In this article, the security performance and quality for image encryption and decryption based on filter bank and the combination between XOR and addition modulo 2^8 have been studied and assessed. The most common security parameters for image encryption and decryption have been employed. The parameters have been used to examine the proposed image encryption scheme with one and two rounds. The parameters include histogram, correlation coefficient, global entropy, block entropy, avalanche effect, number of pixel change rate (NPCR), unified average change intensity (UACI), exhaustive key analysis, and key sensitivity test. The simulation results proved that, the image encryption process passes all these tests. Moreover, it reaches or excels the current state of the arts. So the encrypted image becomes random-like from the statistical point of views after encryption.

Keywords: Image Encryption, Filter Bank, XOR, Histogram, Key Sensitivity.

1. INTRODUCTION

The current progress in computer industry and communications permitted digital multimedia applications like image, file transfer, audio, and video to be distributed over different networking technologies. However, the propagation of these applications over these unreliable and public networks has created a suitable medium for unsafe and uncontrollable distribution [1]. Due to this, protection of these information and data from unauthorized users is becoming more important these days. This can be achieved by using Cryptography. Cryptography is a security technique that requires ciphering or encrypting of data. Encryption is employed to preserve information safe during storage and transmission over communication networks. This process has long been employed by militaries, security organizations and governments to support secret communications and information exchange.

Encryption is the process of converting original multimedia information (i.e., plaintext) into another version usually called a ciphertext to make it hard to be understood excluding those who have knowledge called a key. The resulted ciphertext cannot be accessed and read without decrypting it. Decryption is the process of reconstructing the encrypted information (ciphertext) into its original form. Several security approaches have been proposed to insure the required security and protection of information [2]. Generally, encryption techniques span from simple spatial domain approaches to more complicate frequency domain ones [3]. As a result, exploiting of these security approaches permit users to transmit their information and private data over unsecure communication networks without any fear due to attacks or eavesdropper.

Generally, there are two main kinds of data security systems (i.e., cryptography systems: secret key cryptography and public key cryptography. Secret key cryptography (which is also called symmetric key cryptography) is an approach where both the sender and the receiver know the same the key. Data is encrypted in the sender side by a specific key and the encrypted data is decrypted at the receiver using the same key [4]. However, public key cryptography (which also called asymmetric key cryptography) is an approach where keys work by matching public and private keys [4].

Based on that, multimedia encryption methods must ensure end-to-end security when sharing these applications among users over a variety of communication systems [5]. Image is one of the most important multimedia applications that must be protected and secured against unauthorized access and attacks. That is due to images possess significant applications in numerous fields like medical imaging, videoconferencing, tele-medicine, documentation, and military [6]. Due to this, it is crucial to secure and protect the confidential image information.

Multimedia (i.e., Image) encryption schemes must be carefully designed to protect image content [7]. Most of the existing ciphering algorithms are designed for text encryption. These classical encryption methods are not usually appropriate for image ciphering due to image huge amount of data which requires heavy computations [8]. Therefore, various encryption schemes have been proposed recently for the sake of image encryption only.

In [9] an image encryption method based on block transformation algorithm was proposed. In this paper, the original image is splitted into a random number of blocks. These blocks are then shuffled with the image. This image is encrypted by Blowfish algorithm. The importance of this approach is the use of the seed to generate the random number of block sizes used in image transformation process to produce the shuffled image before encryption. The smaller the block size the better the encrypted image.

An algorithm using permutation was to divide the original image into blocks of 4x4 pixels each to produce lower correlation and higher entropy values [10]. These blocks were distributed over the image and the resulted image was then encrypted using the RijnDael algorithm. The strength of this algorithm was the use of the permutation method to generate a new image very different from the original one before encryption. Using the inverse permutation of the blocks, the original image can be decrypted.

In [11] an image encryption scheme based on improved version of the Advanced Encryption Standard (AES) to increase security level for image encryption. The new proposed approach was based on adjusting the Shift Row Transformation. By this, the modified version of the AES produced results compared to the original AES in terms of reducing the statistical attack opportunities by increasing the security level. In [12] filter bank systems were used as a cryptosystem, in this system, the analysis filter banks were employed to make the encryption process, while the synthesis filter banks were employed to achieve the decryption process.

A Modification on Advanced Encryption Standard (MAES) to improve the level of security and to get enhanced image encryption was proposed in [13]. The experimental results illustrated that higher security levels were obtained compared to the AES encryption algorithm.

The authors in [14] devised an image encryption algorithms using public key encryption called Gödelization. The original image was transformed into a sequence called Godel Number Sequence (GNS). Then the transformed image was compressed using Alphabetic coding (AC). Results of this algorithm showed that it performed efficiently for images encryption but with high processing time for large images.

An image encryption technique using two chaotic systems was introduced in [15]. One is used to generate a chaotic sequence to be transformed into a binary stream by a threshold function. The second chaotic system was employed to build a permutation matrix. The image encryption included randomly modification of the original image pixel values using the binary stream as a key stream. Then, the resulted (transformed) image was encrypted again by the permutation matrix.

Moreover, another image ciphering technique was developed in [16]. This scheme was based on extension of chaotic sequences where chaotic cryptography was used and called a key cryptography. The extended chaotic processes were generated by the n-rank rational Bezier curve which provided high key space and good security level for the encrypted image.

In [17] an encryption scheme was devised using logistic map and cheat image. In this method, a confusion and diffusion approach for image encryption was employed. Logistic map is a discrete chaotic system which was used as secrete key. In addition, a cheat images is selected with size as same as the original image. Then the cheat image and the original image were mixed by a permutation. This cheat image, diffusion and confusion matrices were used to cipher the original image. The standard statistical showed that this image encryption algorithm was robust and secure.

New encryption technique by decomposing the original image into 8x8 blocks was proposed in [18]. These blocks were transformed into frequency domain using the Discrete Cosine Transform (DCT). Then, the higher frequencies DCT coefficients were encrypted by Non-Linear Shift Back Register (stream cipher). The resulted encrypted coefficients are shuffled based on a pseudorandom bit sequence. In addition, the developed algorithm was lossless and selective approach which produced a fast encryption process.

The authors in [19] introduced a new image encryption system using the DNA sequences concepts. This approach was used for improving big image encryption time. DNA sequences were used as main keys. Using the one of the DNA sequence, the plain image pixels were scrambled. Then, another sequence was used to produce DNA template to achieve pixel replacement. Then, the new image was XOR bit by bit with one of the encryption templates generated by DNA sequence. This technique had high security against attacks. Additionally, this technique reduced the encryption time with great extent.

In [20] a scheme was proposed to enhance image encryption techniques based on a logistics algorithm Haar wavelet transform was used to distribute the image and decorrelate its pixels into averaging and differencing components. In this technique, logistic algorithm was used to encrypt the original image. While, the differencing components were compressed using a wavelet transform. The results of the proposed algorithm produced a good and reliable encryption algorithm suitable for real-time image encryption and transmission.

In this paper, a filter bank and addition Mod 2^8 with XOR is used as an image ciphering scheme, in order to enhance the security level and quality of the encrypted images. The paper is organized as follows. Section 2 presents a background of the main parameters that are usually used to assess and analyze image encryption schemes. In section 3, the proposed image encryption scheme is introduced. Section 4 introduces the experimental results and discussion. Section 5 concludes the paper.

2. INVESTIGATION OF SECURITY ANALYSIS PARAMETERS

There is a need for some performance parameters that have to be defined to evaluate and assess any given image encryption scheme. These parameters are discussed in this section.

2.1 Histogram Parameter

It is essential to ensure that encrypted and original images do not have any statistical similarities in order to avoid the outflow of information to attackers. The histogram analysis displays how pixels in an image are distributed. This can be achieved by plotting the number of pixels at each intensity level either for color or gray scale images [21]. The histogram of original image has large sharp goes up then sharply goes down while the histogram of the encrypted image contains uniform distribution which is considerably different from original image [22]. Therefore, the encrypted image histogram should be different from plaintext image histogram [23].

2.2 Entropy Parameter

Entropy is a factor that measures the ambiguity and randomness in a given information or data. For an image, the encryption should reduce the mutual data amongst pixel values and therefore increase the entropy value [24]. A good secure system should satisfy and meet a condition on the information entropy that is the encrypted image should not provide any information about the original image. The entropy value can be obtained using the following equation [25]:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log_2[\frac{1}{p(m_i)}] \text{...} \quad (1)$$

where p(mi) is the probability of occurrence of the symbol mi.

Using equation (1), the ideal value of the entropy is equal 8 assuming that each symbol has equal probability of occurrence and symbols are represented 8-bits each. For a good image encryption algorithm, the entropy value should be very close to the ideal value in order to prevent entropy attack [26].

A block entropy test is sometimes required for more image ciphering analysis in order to provide qualitative and quantitative measures. In this test, the image is divided into B blocks and the entropy is determined for every block (HB) using equation (1) instead of the entropy for the entire image. Hereafter, the mean entropy of the B block entropies is calculated using equation (2) [27]:

$$\overline{H_B} = \sum_{j=0}^{B} \frac{H_j}{B} \text{...} \quad (2)$$

2.3 Correlation Coefficient Parameter

Correlation is one of the main parameters that measure the relationship between two variables to determine how much they are similar. Correlation has values in the range of -1 to +1, where 0 shows no correlation and either -1 or +1 indicates high correlation. If the correlation coefficient equals zero, then the encrypted image and the original image are completely different which means that the encryption image has no features and independent on the original image. If the correlation coefficient equal -1 or +1, this leads that the encrypted image is a negative or positive of the original image, respectively [28].

In the original image, each pixel is greatly correlated with its contiguous pixels [29]. A perfect encryption scheme should generate the encrypted-images with no such correlation in the neighboring pixels. To study the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations, the following equation is used [30]:

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2}.} \text{...} (3)$$

In equation (3), rxy is the correlation coefficient, x and y are the values of two pixels in the same location in the original and encrypted images, respectively, E[.] is the expectation operator of the given pixel values and NxN is the image dimension.

2.4 Diffusion Characteristics

Diffusion is an essential parameter for any ciphering system. Diffusion involves that if any change in the plaintext or the key, this will directly change the ciphertext as well. One bit change in the plaintext image will lead to a significant change in the ciphered image. This is also known as the Avalanche Effect which causes a 50% change in the encrypted image due to a one bit change in the plaintext image. To measure the avalanche effect Mean Square Error (MSE) is commonly used as given in equation (4) [31]:

$$MSE=\frac{1}{MxN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j)-K(i,j)\right]^2 \text{ ....(4)}$$

where I and K are two ciphertext images with keys differ by one bit. M and N are the dimensions of the images. i and j are pixel positions within the images.

To investigate the difference between the original image and the encrypted one, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are usually used. The NCPR calculates the percentage of different pixels between the original and the ciphered images. This can be obtained using equation (5) [32]:

$$NCPR = \frac{\sum_{i,j} D(i,j)}{MxN} x100\% \text{ ....(5)}$$

where D(i,j) is “0” if both images have the same pixel intensities and “1” if they are different.

UACI provides the number of averaged changed intensity between ciphered images. UACI is determined by equation (6) [32]:

$$UACI=\frac{1}{MxN}\left[\sum_{i,j}\left[\frac{\left[I(i,j)-K(i,j)\right]}{255}\right]\right]x\ 100\% \text{ ....(6)}$$

where I, K, M, N, i, and j are as defined in equation (4).

2.5 Key Space Parameter

For an image encryption scheme to be efficient, the key space must be large in order that any attack to be avoided. Additionally, the encryption system should be sensitive to small changes on the security keys. In a good cryptosystem, a wrong decrypted image is produced if there is a small difference in the encryption key. Therefore, an effective image encryption scheme has to be sensitive to resist any change in the keys [33].

There are two ways to test the keys used in encryption process: Key Sensitivity and Exhaustive Key Search. Key sensitivity is necessary for cipher systems. This means that the ciphered image cannot be decrypted correctly in spite of there is a minor change in ciphering and deciphering keys. This will make it secure against brute-force attacks [34]. In the cryptosystem, the key sensitivity is determined by a parameter of sensitivity of the diffusion function. The higher the parameter sensitivity value, the higher the encryption key sensitivity is. Exhaustive Key Search: A cryptosystem must possess a large key space in order to reduce the probability of the attacks on the encryption design. If a designed security system has n-bit key, the exhaustive key requires 2n attempts to discover the key. Based on this, if n is 256 bit, then 2256 trials are needed to get the correct key [35].

3. FILTER BANK WITH ADDITION MODULO 2^8 AND XOR COMBINATION FOR IMAGE ENCRYPTION

In this paper, the filter bank system is used to perform the permutation process, while the *XOR* and addition *Mod* 2^8 is used to perform the substitution process for image encryption [12]. So, the analysis filter bank is employed for image encryption and the synthesis filter bank is employed for image decryption. In this case, the encryption and decryption processes are based on linear circular convolution, which introduces a good permutation layer to achieve the diffusion. To add the required nonlinearity to the cipher to satisfy the confusion principle, *XOR* and addition *Mod* 2^8 is used as shown in Figure 1. To ensure perfect reconstruction during the decryption process, *XOR* and subtraction *Mod* 2^8 is used as shown in Figure 2, where

$\boxed{+}$: The operation of integer Addition mod 2^8, ⊕ : The operation of exclusive-or (*XOR*),

$\boxed{<<<}$: A left rotation and $\boxed{-}$: The operation of integer subtraction mod 2^n.

This combination between *XOR* and addition *Mod* 2^8 and the filter bank provide a strong Substitution – Permutation – Network (SPN). The encryption and decryption process are shown in Figure 3 and Figure 4 for one round cipher, respectively [12]. The image encryption and decryption analysis are performed using one and two rounds of the cipher to examine the security of the image at each stage.

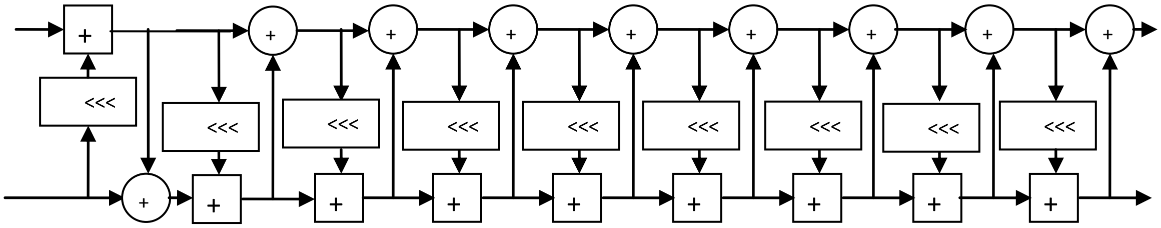


FIGURE 1: Addition *mod* 2^8 and *XOR* Combination.

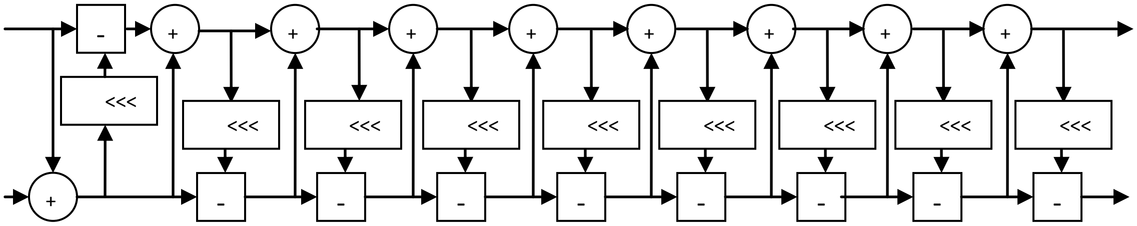


FIGURE 2: Subtraction *mod* 2^8 and *XOR* Reconstruction.

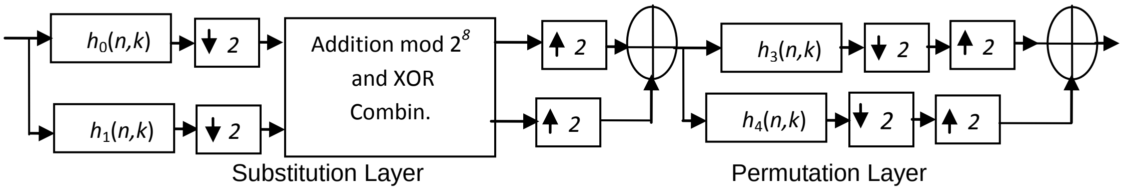


FIGURE 3: One Round for Filter Bank Encryption System.

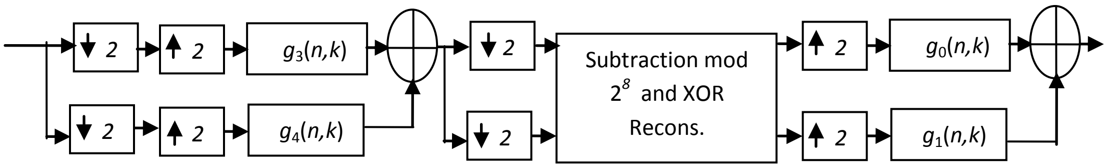


FIGURE 4: One Round for Filter bank Decryption System.

Basically, this cipher has many advantages [12]. Design simplicity, since its implementation based on digital filter design, which offers a high speed implementation in software and hardware. Also, it offers a high security level using small number of rounds. Moreover and the most important, it can introduce the scalability to the system, as it can deal with different length of key or plaintext which can be adjusted according to a particular encryption application.

4. SIMULATION RESULTS AND SECURITY ANALYSIS

In this section the security of the image encryption scheme will be evaluated for one and two round filter bank system using many parameters.

4.1 Histogram Analysis

To improve the security of the encrypted image, it is essential to ensure that, there is no statistical similarity between the original and encrypted images. The histogram is used to clarify the image pixels distribution. In this paper, the histograms for two images (Cameraman and Baboon images) and their encrypted images with one and two rounds are analysed as shown in Figure 5 and Figure 6. Note that, the histograms for the original images are not uniformly distributed, rather than, contain large sharp rises followed by sharp declines. While the histogram distributions for the encrypted images are uniformly distributed, and significantly different from the histograms of the original images. So there are no statistical similarity between the encrypted images and the original images. As a result, the encrypted images are random-like.

4.2 Information Entropy

The global entropy is employed to express the uncertainties of the system. The global information entropy for truly random gray scale source is 8. Therefore, the global entropy of the encrypted image should be very close to 8 bits to ensure its security. To study the global entropy attack, two images are encrypted using one and two rounds with different keys. Then the global entropies are calculated using equation (1) and the results are summarized in Table 1. The results in Table 1 are very closed to the theoretical value (8 bit), which means that, the information leakage in the encryption scheme is negligible, so it is secure against the entropy attack.

	Baboon Image		**Cameraman Image**	
Key	One Round	Two Rounds	One Round	Two Rounds
Key One	7.9937	7.9971	7.9931	7.9975
Key Two	7.9936	7.9975	7.9934	7.9973

TABLE 1: Global Entropy Results for Encrypted Baboon and Cameraman Images.

Another entropy attack called block entropy can be used to measure the local entropy over image blocks. To calculate the block entropies for the encrypted images, a randomly 100 non-overlapping blocks from the encrypted images have been selected. After that, the entropy for each block is calculated and recorded and averaged to find the block entropy using equation (2). The calculated values the block entropies are summarized in Table 2. It is clear that, the block entropies of the encrypted images with different keys are higher than the minimum theoretical critical block entropy for one and two rounds cipher. So, the encrypted images become random-like after encryption process.

	Baboon Image		**Cameraman Image**	
Key	One Round	Two Rounds	One Round	Two Rounds
Key One	7.1743	7.1898	7.1805	7.1907
Key Two	7.1798	7.1909	7.1735	7.1888

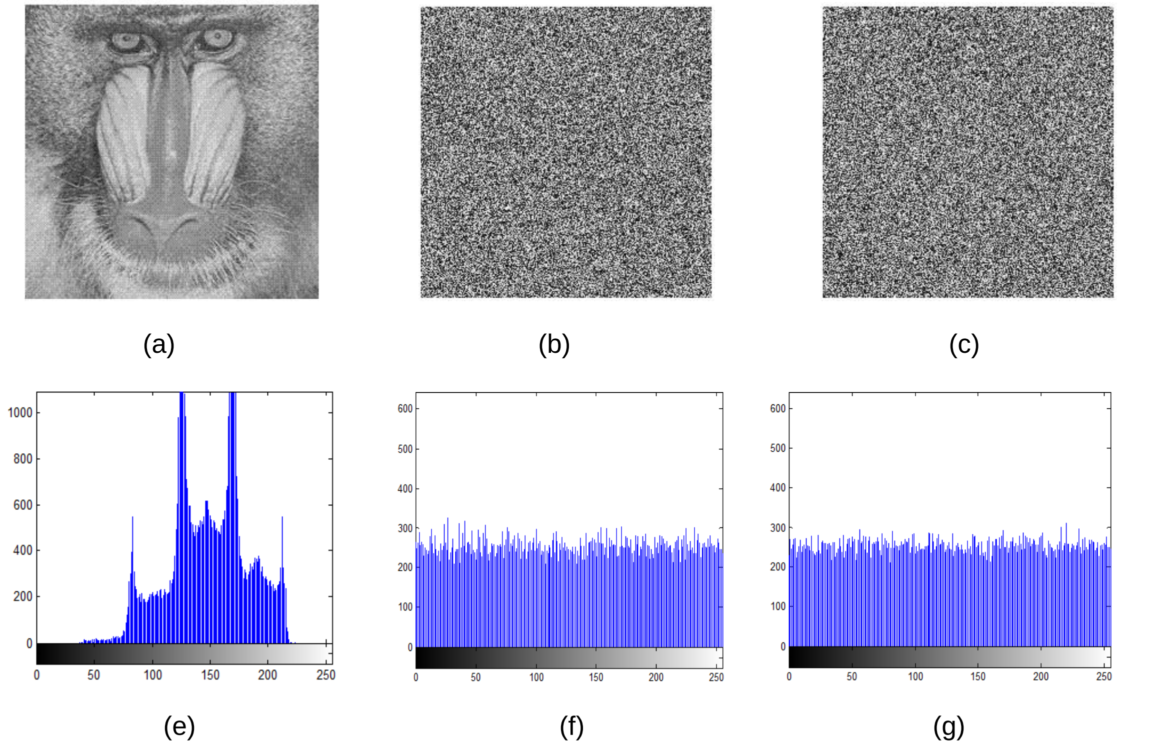
TABLE 2: Block Entropy Results for Encrypted Baboon and Cameraman Images.

4.3 Correlation Coefficients Analysis

To measure the relationship between the original and the encrypted images, the correlation coefficient can be utilized. It determines the encryption quality. The maximum value for the correlation coefficient is one; in this case the two variables are the same. So the correlation coefficient should be vey closed to zero to get a good encryption quality. For image encryption analysis, the correlation coefficient can be calculated between the adjacent pixels in three directions (horizontal, vertical and diagonal). This test has been carried out for Cameraman and Baboon and their encrypted images of size 256 x 256 pixels. In this test, 1000 pairs of the two adjacent pixels are randomly selected in all three directions from the images. Then, the correlation coefficients are calculated using equation (3). The results in Table 3 indicate that, after the encryption process, the highly correlated images are completely broken in all directions. Note that, before encryption, the horizontal correlation coefficient for Cameraman image is 0.9282, but after encryption using one round it becomes 0.0139, and 0.0021 after two rounds. So, the highly correlated horizontally adjacent pixels before encryption become uncorrelated after the encryption process. The same results are obtained in diagonal and vertical directions as mentioned in Table 3. Accordingly, the encryption quality is good.

	Original Images		**Encrypted Baboon Image**		**Encrypted Cameraman Image**	
Correlation Coefficients	Baboon Image	Cameraman Image	One Round	Two Rounds	One Round	Two Rounds
Horizontal	0.7103	0.9282	0.0256	-0.0062	0.0139	0.0021
Vertical	0.5966	0.9644	0.0341	0.0076	-0.0561	0.0215
Diagonal	0.6225	0.9116	-0.0239	0.0087	0.0141	-0.0040

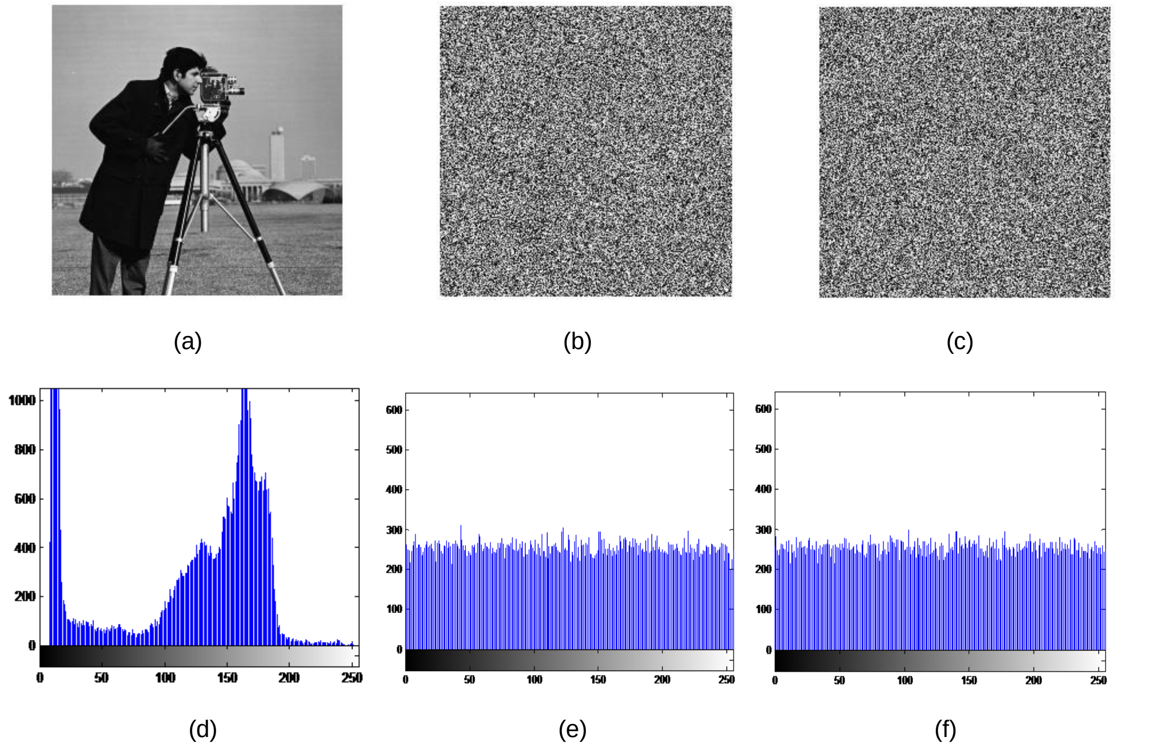
TABLE 3: Correlation Coefficients Results.



(a) (b) (c)

(e) (f) (g)

FIGURE 5: (a) Original Banoon image. (b) Encrypted image using one round. (c) Encrypted image using two rounds. (d) Histogram of the Baboon image. (e) Histogram of encrypted image using one round. (f) Histogram of encrypted image using two rounds.



(a) (b) (c)

(d) (e) (f)

FIGURE 6: (a) Original Cameraman image. (b) Encrypted image using one round. (c) Encrypted image using two rounds. (d) Histogram of the Cameraman image. (e) Histogram of encrypted image using one round. (f) Histogram of encrypted image using two rounds.

4.4 Diffusion Characteristics

4.4.1 Avalanche Effect

The avalanche test examines the security of the encrypted image based on a small change of the original image (usually one bit differ) using the same key. To ensure the security, any small change in the original image should give a significant change in the encrypted image. In this paper, two images have been encrypted using the same key. After that, the original images with one bit differ for each has been encrypted with the same key. To check the influence of one bit change in the original images, the MSE is calculated using equation (4). The results in Table 4 ensure that, the MSE > 30 dB [36] using one or two rounds, this means, a slight difference in the original images yields a huge change to the encrypted images which certifies the diffusion principle.

Encrypted Image	One Round	Two Rounds
Baboon Image	40.11 dB	40.36 dB
Cameraman Image	40.14 dB	40.35 dB

TABLE 4: MSE Results.

4.4.2 NPCR and UACI

To examine the security of the image encryption scheme against the differential attack, NPCR and UACI can be employed. NPCR measures percentage of the number of different pixel to the total number of pixels. UACI computes the average intensity of the differences between the images. So to examine the influence of one bit change, these tests are performed on Baboon and Cameraman images. Simulation results obtained in Table 5 show that, the encryption scheme using number different of rounds is very sensitive to a small change in the original images. Note that, the higher the value of NPCR and UACI, the better the encryption scheme. As a result a strong diffusion has been done, and the encrypted images are very random- like. Then the efficiency of the differential attack is vanished and practically useless.

Encrypted Image	One Round NPCR	Two Rounds NPCR	One Round UACI	Two Rounds UACI
Baboon Image	99.55	99.67	33.38	33.61
Cameraman Image	99.59	99.66	33.35	33.60

TABLE 5: NPCR and UACI Results.

4.5 Key Space Analysis

A strong image encryption scheme must be very sensitive to the key. To evaluate the key space analysis two methods are used.

4.5.1 Exhaustive Key Analysis

Basically the proposed cipher is a scalable cipher, so it can deal with different key length based on the required security level. In this paper the minimum key length images is 128 bit. So, if an attacker uses 1000 MIPS computer to break the key using the brute force attack, the attacker needs

$$\frac{2^{128}}{1000\times10^{6}\times60\times60\times24\times365} > 10.79\times10^{21} \text{ Years}$$

This is very long time period which is infeasible [30].

4.5.2 Key Sensitivity Test

To test the sensitivity of the encrypted decrypted image due to a minor change of the key, key sensitivity test can be used. The key sensitivity can be addressed with respect to two portions:

1) Encryption: if the same image (P) is encrypted using key 1 (K1) and key 2 (K2) which are different in one bit only. Then how is the difference between the two encrypted images (C1 and C2).

2) Decryption: if the encrypted image (C1) is decrypted using two encryption keys (K1 and K2), which are different only in one bit. Then how is the difference between the two decrypted images (D1 and D2).

Suppose that, there are three keys (K1, K2 and K3) where all differ only in one bit. Then, the encryption process has been performed for the images (Baboon and Cameraman) using one and two rounds. Figures 7 and 8 show the sensitivity of the encrypted and decrypted images using one or two rounds due to the small change of the key. As a result, the confusion property is satisfied over the encrypted images using both one and two rounds. The corresponding percentage differences between two encrypted images with one bit differ in the key for Baboon and Cameraman images are calculated as depicted in Table 6.

Encrypted Image	One Round	Two Rounds
Baboon Image	99.5850%	99.6560%
Cameraman Image	99.5770%	99.6600%

TABLE 6: Difference of When Keys Differ by One Bit Results.

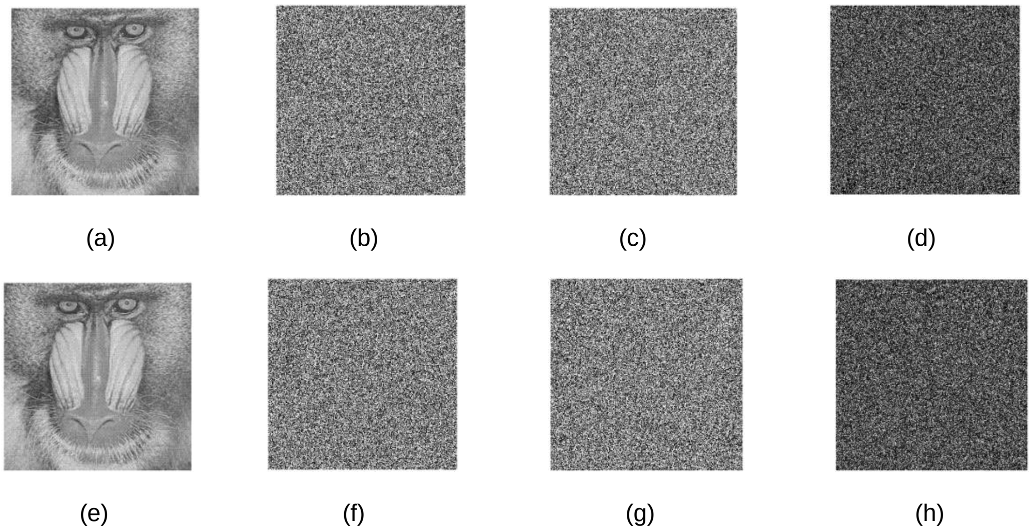


FIGURE 7: (a) Original Baboon image (P). (b) Encrypted image using K1 with one round (C1). (c) Encrypted image using K2 with one round (C2). (d) Encrypted images difference |C1 – C2|. (e) Decrypted image (C1) using K1 gives (D1). (f) Decrypted image (C1) using K2 gives (D2). (g) Decrypted image (C1) using K3 gives (D3). (h) Decrypted images difference |D2 – D3|.

4.6 Statistical Comparative Evaluation Results

To evaluate the security of image encryption using two rounds filter bank cipher, it is important to compare it with other popular image encryption ciphers. In this paper, the simulation results for two rounds cipher are compared with two image encryption schemes; namely, AES and Compression Friendly Encryption Scheme (CFES) which were analyzed in [21]. The values in Table 7 demonstrate that, the two rounds of the proposed filter bank cipher is stronger than

CFES; in addition it has the same results as AES and some results better than the AES results. Moreover, the filter bank cipher supports simpler implementation and scalability, where the other ciphers do not provide the scalability.

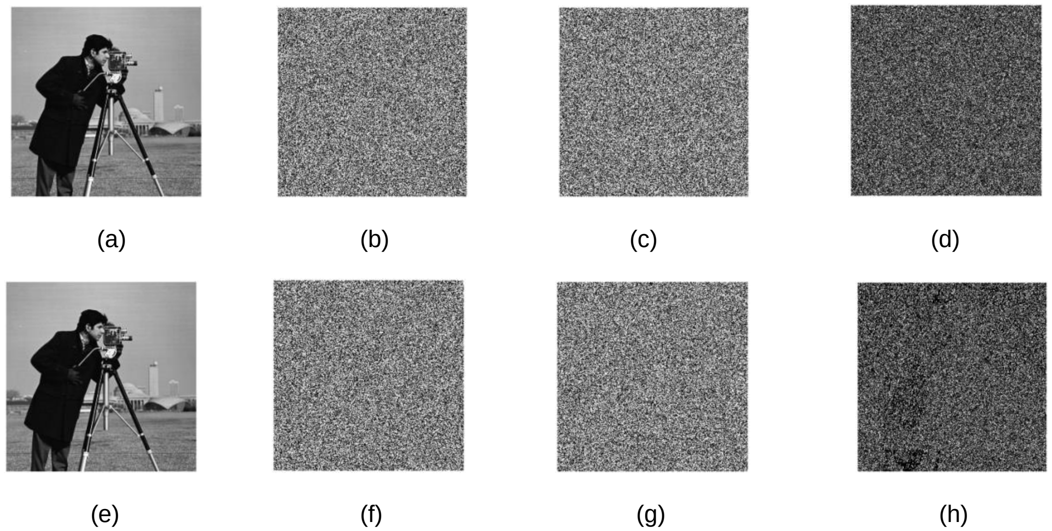


FIGURE 8: (a) Original Cameraman image (P). (b) Encrypted image using K1 with two rounds (C1). (c) Encrypted image using K2 with two rounds (C2). (d) Encrypted images difference |C1 – C2|. (e) Decrypted image (C1) using K1 gives (D1). (f) Decrypted image (C1) using K2 gives (D2). (g) Decrypted image (C1) using K3 gives (D3). (h) Decrypted images difference |D2 – D3|.

	Encrypted Baboon Image			Encrypted Cameraman Image		
	AES	**CFES**	**Proposed**	**AES**	**CFES**	**Proposed**
Horizontal Correlation Coefficient	-0.0370	0.9547	-0.0062	-0.0067	0.9522	-0.0021
Vertical Correlation Coefficient	0.0107	0.0611	0.0076	0.0504	0.0124	0.0215
Diagonal Correlation Coefficient	-0.0419	-0.0025	0.0087	-0.0156	0.0202	0.0040
Global Entropy	7.9973	7.1404	7.9975	7.9975	7.1455	7.9975
Block Entropy	-	-	7.1909	-	-	7.1907
NPCR	99.62	99.09	99.67	99.60	99.12	99.66
UACI	33.36	15.39	33.61	33.53	15.49	33.60
MSE	40.34 dB	33.31 dB	40.36 dB	40.39 dB	33.86 dB	40.35 dB
Key Sensitivity	99.6506%	99.1882%	99.6560%	99.5880%	99.2554%	99.6600%

TABLE 7: Parameters Evaluation Comparison with AES and CFES.

5. CONCLUSIONS AND FUTURE WORK

In this paper, the image encryption quality using filter bank with XOR and addition *Mod* 2^8 combination cipher with one and two rounds are evaluated and analyzed using many evaluation parameters. The evaluation parameters are histogram analysis, correlation coefficient, global entropy, block entropy, avalanche effect, NPCR, UACI, exhaustive key analysis, and key sensitivity test. The overall results proved the security of the proposed algorithm. The simulation results for histogram showed that the distribution of the encrypted image is uniform and completely different from the histogram of the original image. In correlation coefficient analysis, the correlated adjacent pixels of the original images are completely distributed in the encrypted image with very small correlation coefficient in all directions (horizontal, vertical and diagonal), so the highly correlated images are uncorrelated after encryption. The global and block entropy are very close to ideal, so the encrypted image represent random – like image. The diffusion characteristics for the encryption scheme were proved through avalanche test, NPCR and UACI. The key sensitivity results showed that image encryption and decryption are very sensitive to any minor change in the key. Accordingly, the image encryption process passes all these tests; as a result, the encryption process is considered as a strong and robust process to resist many existing cryptography attacks and cryptanalysis technique. Also, the results obtained in this paper are compared with other image cipher schemes; the proposed cipher shows it's leading. To ensure the image encryption security and immunity against cryptanalysis technique, it is better to use two rounds filter bank with *XOR* and addition *Mod* 2^8 combination cipher even the result for one round showed good security. In future work, the performance analysis for audio and video signal will be evaluated and investigated using the proposed cipher.

6. REFERENCES

[1] F. BORKO, S. DANIEL, and M AHMET.Fundamentals of multimedia encryption techniques. Multimedia Security Handbook, 2004.

[2] H. AHMED, H. M KALASH, and O. S FARAG ALLAH.: Encryption analysis of the rc5 block cipher algorithm for digital images. Menoufia University, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt 2006.

[3] H. RATHOD, M. SISODIA, and S SHARMA." A review and comparative study of block based symmetric transformation algorithm for image encryption." International Journal of Computer Technology and Electronics Engineering (IJCTEE) 1(2), 2011.

[4] N. FERGUSON, B. SCHNEIER, and A KOHNO. Cryptography engineering. 2nd edition, John Wiley & Sons, 2010.

[5] A. GUPTA, N. JOSHI and C. NAGAR, "A review new symmetric image encryption scheme based on correlation pattern." International Journal on Emerging Technologies 3(1): 2012, pp 102-104.

[6] K. MILOZŠ, "Qualitative aspects of image applications in multimedia technology." 17th IEEE International Conference on Radioelektronika, April 2007, Prague, pp.1 – 11.

[7] B. FURHT and D. KIROVSKI. Multimedia security handbook. CRC Press, Boca Raton, Florida, 2005.

[8] P. KARTHIGAIKUMAR and S. RASHEED. "Simulation of image encryption using AES algorithm." IJCA Special Issue on Computational Science - New Dimensions & Perspective 2011.

[9] M. A. BANI YOUNES and A. JANTAN. "Image encryption using block-based transformation algorithm." IAENG International Journal of Computer Science, 35(1) 2008a.

[10] M. A. BANI YOUNES and A. JANTAN "An image encryption approach using a combination of permutation technique followed by encryption." International Journal of Computer Science and Network Security (IJCSNS), 8(4) 2008b.

[11] S. H. KAMALI, R. SHAKERIAN, M. HEDAYATI, and M. RAHMANI. "A new modified version of advanced encryption standard (aes) based algorithm for image encryption." IEEE Transactions on Electronics and Information Engineering, 2010a, 1:141-145.

[12] S. SARAIREH and M. BENAISSA. "A scalable block cipher design using filter banks over finite fields." In Acoustics Speech and Signal Processing (ICASSP), IEEE International Conference, Dallas, TX, USA 2010.

[13] S. H. KAMALI, R. SHAKERIAN, M. HEDAYATI, and M. RAHMANI. "A new modified version of advance encryption standard based algorithm for image encryption." International Conference in Electronics and Information Engineering (ICEIE) 2010b.

[14] B.V. RAMA DEVI. "A novel encryption method for the secure transmission of images." International Journal on Computer Science and Engineering, 2(9): 2010, pp 2801-2804.

[15] H. XIAO and G. ZHANG. "An image encryption scheme based on chaotic systems." IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian 2006.

[16] Y. ZHANG. "Image encryption using extended chaotic sequences." IEEE Transactions International Conference on Intelligent Computation Technology and Automation, 2011a pp: 143-146.

[17] Y. ZHANG. "Image encryption with logistic map and cheat image." 3rd International Conference on Computer Research and Development (ICCRD), 2011b, 1: 97 – 101.

[18] L. KRIKOR, S. BABA, T. ARIF and Z. SHAABAN. "Image encryption using DCT and stream cipher." European Journal of Scientific, 32(1) 2009, pp47-57.

[19] Z. ZHOU SHIHUA, Z. QIANG, and W. XIAO-PENG. "Image encryption algorithm based on DNA sequences for the big image." International Conference on Multimedia Information Networking and Security, 2010, pp 884-888.

[20] N. SETHI and D. SHARMA. " A new cryptology approach for image encryption." 2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC), 2012, pp 905 – 908.

[21] J. AHMAD and F. AHMED. "Efficiency analysis and security evaluation of image encryption schemes." International Journal of Video and Image Processing and Network Security, 12(4), 2012.

[22] A. JOLFAEI and A. MIRGHADRI. "Image Encryption Approach Using Chaos and Stream Cipher." Journal of Theoretical and Applied Information Technology, 2010a.

[23] A. JOLFAEI and A. MIRGHADRI. "Survey: image encryption using A5/1 and W7." Journal of Computing, 2(8), 2010b .

[24] S. E. BORUJENI, and M. ESHGHI. "Chaotic image encryption design using tompkins-paige algorithm." Hindawi Publishing Corporation, Mathematical Problems in Engineering, Article ID 762652, 2009.

[25] U. PANDEY, M. MANORIA, and J. JAIN. "A novel approach for image encryption by new m box encryption algorithm using block based transformation along with shuffle operation." International Journal of Computer Applications, 42(1), 2012.

[26] R. ENAYATIFAR. "Image Encryption Via logistic map function and heap tree." International Journal of Physics Science, 6(2) 2011.

[27] S. RAKESH, A. AJITKUMAR, B. SHADAKSHARI, and B. ANNAPPA. "Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping." International Journal on Cryptography and Information Security (IJCIS), 2(1) 2012.

[28] B. AÏSSA, D. NADIB, and R. MOHAMED. "Image encryption using stream cipher based on nonlinear combination generator with enhanced security." NEW TRENDS IN MATHEMATICAL SCIENCES, 1(1) 2013, pp 18-27.

[29] A. N. PISARCHIK and M. ZANIN. "Image encryption with chaotically coupled chaotic maps." Physica D, 237(20): 2008 pp 2638-2648.

[30] I. ELASHRY, O. ALLAH, A. ABBAS, S. RABAIE, and F. EL-SAMIE. "Homomorphic image encryption." Journal of Electronic Imaging, 18, 2009.

[31] Z. HEGUI, L. XIAOJUN, T. QINGSONG, Z. XIANGDE, and Z. CHENG. "A new chaos-based image encryption scheme using quadratic residue." IEEE International Conference on Systems and Informatics (ICSAI), 2012, pp 1800-1804.

[32] C. K. HUANG, and H. H. NIEN. "Multi chaotic systems based pixel shuffle for image encryption." Optical communications, 282, 2009, pp 2123-2127.

[33] A. DIACONU, and K. LOUKHAOUKH. "An improved secure image encryption algorithm based on rubik's cube principle and digital chaotic cipher." Mathematical Problems in Engineering, Hindawi Publishing Corporation, 2013.

[34] S. LIAN, J. SUN, and Z. WANG. "Security analysis of a chaos-based image encryption algorithm." Physics Letters A 35, 1, 2005, pp 645-661.

[35] A. M. RIAD, A. H. HUSSEIN, H. M. KASEM, and A. ABOU EL-AZM. "A new efficient image encryption technique based on arnold and idea algorithms." International Conference on Image and Information Processing (ICIIP 2012), 46, 2012, Singapore.

[36] Z. LIEHUANG, L. WENZHUO, L. LEJIAN, and L. HONG. "A novel image scrambling algorithm for digital watermarking based on chaotic sequences." International Journal of Computer Science and Network Security, 6(8B), 2006, pp 125–130.

The Impact of Customer Knowledge on the Security of E-Banking

Nabeel Zanoon *dr.nabeel@bau.edu.jo*
Aqapa College , Balqa Applied University
Aqapa, Jordan

Natheer Gharaibeh *nkgharaibeh@bau.edu.jo*
Ajloun College , Balqa Applied University
Ajloun, Jordan

Abstract

In this paper one of the most affective factors on security of e-banking will be discussed, by accepting the use of information technology for the execution of the Traditional e-banking, As we know that e-banking is done online and the customers are considered the active element and the other party in e-banking operations. So if the level of customer knowledge in the use of IT ص low, then this points that customers are not professional in the execution of the traditional e-banking using IT , furthermore this create flaws in the security of e-banking by facilitating the sneaking into the personal information and distrust in customer confidence of the e-banking security. which leads to reject the use of technology in e-banking, And this is what will be discussed in this paper by offering some security gaps which is resulting from the low level of customer knowledge in information technology, and that will be studied through Technology Acceptance Model and In light of this we will suggest some solutions.

Keywords: Trust, E-Banking, Customer Knowledge, Information Technology, Technology Acceptance Model.

1. INTRODUCTION

Due to the important role of commercial banks in this era both in terms of economic or social factors, the need has increased to use modern technology of computers, e-service systems electronic banking basic and secondary rather than traditional information systems, and as a result started the need to learn scientific methods to study these systems and can be introduced and implemented in order to make them more efficient , effective , accurate and reliable information for the beneficiaries.

The new information technology (IT) is turning into the most important factor in the future development of banking, influencing banks marketing and business strategies. In recent years, the adoption of e-banking began to occur quite extensively as a channel of Distribution for financial services due to rapid advances in IT and intensive competitive banking markets [1] While the use of online banking services is fairly new experience to many people [2] Carry with them the underlying assumption that designs should encourage exploration or, at least, allow for a trial-and-error approach to learning how to use systems. However, for e-banking and other security-sensitive systems, a trial-and-error approach is generally not acceptable because a security breach caused by an error may be exploited by an attacker before the error is revoked by the user [3].

User adoption of a technology has become a crucial measure for the success of that technology [4] For carrying out Internet banking properly, a basic knowledge of computers and the Internet is required, which limits the number of people willing to gain this facility. Many people, who are not familiar with computers and the Internet, often find it difficult to use Internet banking. Therefore, for beginners, Internet banking is really time-consuming. In addition to this, people also find a difficulty in trusting a completely mechanized system like Internet banking, in case of financial matters. In many instances, a simple mistake, like clicking a wrong button, may create a big problem [5].

Technology is evolving every day and in almost in every aspect but not everything that is coming in the way is being accepted. Before anyone adopt a technology, all the Information about the technology will be collected and combined to develop a belief about using the technology and that belief will in turn make the individual to accept or reject the technology [6] when users are satisfied with a technology the technology adoption is likely to be higher. In addition, Technology Acceptance Model (TAM) asserts that users'. Decision to use a technology depends on two factors: perceived ease of use and perceived usefulness [7]. Understanding users' attitude towards the adoption of new technologies has proved to be one of the most challenging issues in technology adoption literature [8].

The increasing number of internet banking users indicates that the internet backing's acceptance level has improved. Internet baking's acceptance level can be influenced by several factors. One model that is often used to describe acceptance level of information technology is TAM (Technology Acceptance Model) (Davis, 1989).perceived usefulness and perceived ease of use is believed to be the basis in determining acceptance of information technology. Both of these factors influence intention to use information technology before it can finally create the actual usage in daily life [9].

This paper will discuss affective factors on security of e-banking in addition to the main factors that affect e-banking security; the remainder of this paper is structured as follows: Section 2 describes Knowledge and skills of IT. Section 3 shows the threats to the security of e-banking.. Section 4 discusses Technology Acceptance Model (TAM) which used in this research. our preposition to solve the problem and RESEARCH MODEL are given in section 5 , and we conclude and present future work in Section 6.

2. KNOWLEDGE AND SKILLS OF IT

Knowledge and skills improve people's ability to meet their needs, extend the variety of options open to them in all areas of their lives. The skills people possess can also enhance their sense of self-worth, security and belonging. We live in a society where access to information and proficiency with technology are becoming more important. An inclusive society will increasingly require everybody to have high levels of knowledge and skills. Knowledge and skills include education and training, as well as abilities gained through daily life [10] Individuals who are skilled and always using the internet significantly affect the acceptance of Internet banking services. Users who are knowledgeable in using computers and the Internet will influence them to use Internet banking services [11]

Internet banking helps banks in cost saving, increase customer base, enable mass customization for e-Business services, extend marketing and communication Channel, search for new innovation services, and explore and develope of non-core business. However, customers' ability to subscribe to the Internet-base banking services depend on several factors such as user-friendly interface, level of Internet experience, types of services provided, (for example e-mail, file transfer, news, online financial services, shopping and multimedia services), attitude and perception, access and delivery time and experience with the Internet [12]

3. THREATS TO THE E-BANKING SECURITY

Online banking is a main step for many customers as it is popular for customers to just go onto their computers at home or work and log onto the online banking site, the customers will then be able to exchange money from one account to another and pay bills with a press of a button. As more technology for online banking is increasing and the security seems to be getting tighter there are still possibilities that the accounts that you are going on can get hacked. There are always chances to reduce the risk of fraud [13].Each and every time you log onto the internet your computer is at risk of various threats with the aim of getting your personal details and accessing your money. Behind the scenes we use various security measures to ensure that your transactions and personal information are protected and safe. However, you as a customer can also play a big part in protecting your banking and personal information. The first step in that process is to understand the main threats to your computer [14]Unawareness of threat - If users are unaware that their personal information is actively being targeted by criminals, they may lack the standpoint needed to identify phishing threats and may not take the proper defense when conducting online activities[15].

Many factors affecting why customers are concerned about their online banking security. The same factors are also driving the need for enhanced authentication for online banking solutions. These factors include the growing number of phishing attacks, the increased usage of pharming and malware, and widespread data security breaches [16]

3.1 Cookies

A cookie is a small chunk of data generated by a web server and stored in a text file on your computer's hard disk. Cookies allow a web site to store information on a client computer for later retrieval [17] furthermore Cookies are used as an authentication tool to allow users automatically access certain web sites without asking the server to look at authorized users at the database .the user's log in name and password are stored in the cookie so that the user can access a subscribed web site automatically each time the user clicks on the web page. The use of cookies has privacy concerns because cookies contain information about the URL of the web page you accessed [18]. Therefore Cookies have become a source of privacy concern in recent years .as with most technologies in the computer industry ,this reputation has been earned by the misuse of the technology more than the technology itself. Many web browsers have the use of cookies enabled by default (without user caution), and many people have taken advantage of this situation by profiling customer tendencies, collecting unnecessary personal information, and so on .the semantics of cookies are fairly well designed for the task they are intended to accomplish. The abuse, however, has resulted in cookies having a rather negative connotation [19].

3.2 Phishing

The term 'phishing' has its origins from the analogy that identity thieves who are using lures usually in the form of e-mails to 'fish' for passwords and financial data from the 'sea' of Internet users, [20] Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures [21] Phishing threat, instead a comprehensive education and awareness program should be devised to go hand in hand with other technical countermeasures to minimize the impacts of phishing to the Internet banking sector and regain users trust[22] a phishing website is a broadly launched social engineering attack that attempts to defraud people of their personal information including credit card number, bank account information, social security number and their personal credentials in order to use these details fraudulently against them. Phishing has a huge negative impact on organizations' revenues, customer relationships, marketing efforts and overall corporate image [23].

3.3 Key Logging

Keystroke logging which is often called key logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored [24] a keystroke logger on a consumer's personal computer. It may create security risks if it exposes communication channels to hackers. Spyware also may adversely affect the operation of personal computers, including slowing processing time and causing crashes, browser capturing, home page resetting, installing dialers, and the like. These harms are problems in themselves, and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce [25] unfortunately for consumers; key loggers are becoming very sophisticated. Once on a PC, they can track websites visited by the user and only log the keystrokes entered on the websites that are of particular interest to the cyber criminal; for example online banking websites [26] the principal problem with internet banking is that customers use acknowledged untrusted systems in gaining access to the bank internet facilities Trojan horse key loggers can, as has been identified in the scarfo case be lurking on a customer's own computer collecting relevant information which can later be used for nefarious activity[27].

3.4 Padlock

A common mistake made by end users believes that their online banking session is perfectly safe when they use an SSL connection. Security experts continually state that everything is safe if there is a yellow padlock symbol in the browser window But SSL is designed as a secure tunnel from the end user computer to the bank mainframe and does not protect the end points such as the end user’s computer [28]

FIGURE 1: The Yellow Padlock Symbol as Displayed in Internet Explorer.

External trust seals are items of a general nature that are used to engender trust, such as the VeriSign symbol and the padlock representing security. Internal regulatory seals include the banks’ own policy declarations, and corporate branding. The wide-ranging nature of the referenced phenomena demonstrates the differing ways in which the subjects are choosing to interpret the signs of trust embedded within the e-banking home-pages [29].

4. TECHNOLOGY ACCEPTANCE MODEL

The technology acceptance model (TAM), developed by Davis, F., et al., (1989),is one of the most widely used and influential models in the field of information systems, technology and services. It has been validated to be powerful as a framework to predict user acceptance of new technology. The goal of TAM is to predict information system acceptance and diagnose design problems before users have any noteworthy experience with the system. TAM measures the determinants of computer usage in terms of perceived usefulness and perceived ease of use. TAM has been effective in the modeling of acceptance of IT and has received extensive experimental support through the studies predicting the use of information systems [30] TAM has proven to be a theoretical model in helping to explain and predict user behavior of information technology [31] User acceptance remains a obstacle to the success of new information technologies (IT). In an attempt explain this, Davis (1989) a thorough understanding of the TAM model may help us to analyze the reasons for resistance toward the technology and would further enable us to take efficient measures to improve user Acceptance of the technology. TAM used in several IS studies and proved useful determining technology acceptance, especially to explain computer usage behavior. Technology Acceptance Model (TAM) has been widely used to predict user acceptance and use based on perceived usefulness and ease of use [32]. In our research we will update the TAM into more suitable model for security of e-banking , we will show that in the next section in figure 2.

5. RESEARCH MODEL AND HYPOTHESES

When the information technology began the development of information systems, the users believes it is difficult to deal with these systems and the prospect of facing a problem in the daily implementation of e-banking. So, we must take into account the fact that the failure use of information technology in the application of banking are often due to lack of users acceptance and the lack of knowledge in the use of banking applications using information technology, the lack of knowledge indicator leads to falling into some flaws This flaws and gaps are recorded against the negative use and because it deals with the systems that contains financial values, and this generates among customers who are not familiar with information technology fears of using e-banking, and these fears pointer to the lack of confidence in the application of e-banking.

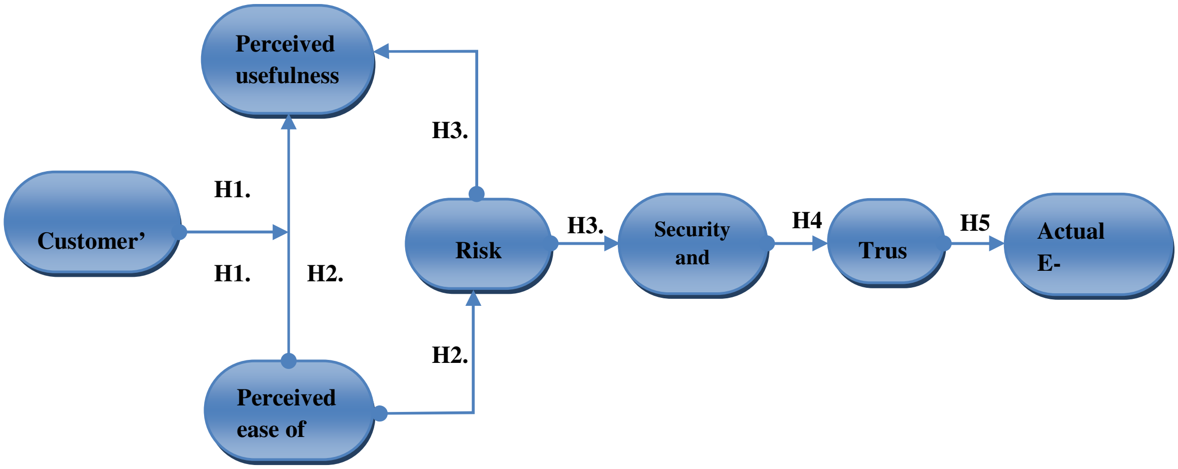


FIGURE 2: Research Model (Technology Acceptance Model).

TAM shows the situation of the user to the technology in general, our updated model shown in figure 2 adds several factors such as the extent of knowledge of users in the use of e-banking , risk factor that affects the security and confidence factor, as all these factors affect the acceptance of the use of technology in e-banking . The study used a model to accept an expanded technology shown in the figure 2 so as to examine the factor customer knowledge in information technology affecting the use of IT in the banking applications. Accordingly, the following subsections will express the propositions emerged from our model:

5.1. Customer's Knowledge of IT

In general the customers know the low-level techniques lead to the appreciation of the potential added value that is inherent in the technology. Experience with the use of the computer, such as the practice of some online business, correspondence and communicate with friends, may affect customers' attitudes towards online banking [33] Therefore the skills to use computers and the Internet for customers of the basics of online banking and this, some countries in Europe worthwhile to develop individual abilities and skills to use the Internet users have Increasing the skills of the individual lead to a trend in most of the application of online banking services [34] In addition, the Some users who do not have a good knowledge about the security risks of online banking, although they are aware of the risks, or perhaps because they know that there is a danger or just ignore the risk [35] In spite of this, people want to use and benefit of technology, including, but cannot ignore the effects and risks that may result from it, however, remains lack of knowledge of an obstacle to the use of technology [36] Although the electronic banking process enables customers to control banking operations. Clients such as students, who are familiar with the internet, you should not find electronic banking processes are complex, however, and efficiency. Customers can also find some difficulties with the service and personal computers and the Internet (such as security and safety concerns complexity, and distrust of regulations and standards, and traditional principles) [37].

H1a: The level of knowledge a customer's has about IT affects on Perceived ease of use.

When the level of customer's knowledge in information technology is high this will lead to high understanding of the banking procedures and doing them faster and thus will be reflected positively on the ease of use, leading to the benefit from the use of information technology in the Daily banking practices.

This proves that the customer will evaluate e-banking easy to use if they have experience of computer use .The experience on the use of computers owned by the customer, will make customers more familiar in using e-banking . Customers who have experience on the use of computers will be easier in the use of e-banking, compared with customers who do not have experience on the use of computer [38].

H1b: The level of knowledge a customer's has about IT affects on perceived usefulness.

5.2 The Perceived Ease of Use and Perceived Usefulness

Earlier research suggested two determinants that are especially important. First, people tend to use or not use an application to the extent they believe it will help them perform their job better. We refer to this first variable as perceived usefulness. Second, even if potential users believe that a given application Is useful, they may, at the same time [39]

For studying the acceptance of e-banking, the general TAM is inadequate because the technology used and the transaction environment in e-banking are different from that of conventional IT and the normal business environment. Before accepting e-banking services, users should be aware about benefits, security issues and the risk associated with it [40]. Perceived ease of use was observed to have no direct effect on behavioral intention but have an indirect effect influence on behavioral intention through its effect on perceived usefulness and perceived risk this result probably is caused by the fact that a big portion of our sample consists of mature internet banking user who are not facing problems in using the system given the usefulness of the system properties .the impact of Perceived ease of use on perceived risk is appeared to be significant meaning that the system friendliness Lowers customers fears about the problems that may have about their transactions security and personal privacy .finally perceived risk was observed to negatively affect usage continuance[41].

H2 a: Perceived ease of use effect on perceived usefulness.

H2 b: Perceived ease of use effect and create security risks.

When customers believe in ease of use of information technology in the implementation of banking, this is indicator to the absence of any risks that may arise from doing business banking, hence the customers underestimate the risks that threaten the security of banking which leads to the low probability of risk through belief in ease of use. Accordingly customers reassure and do not take any degree of security interest and this may lead to security threats

5.3 Perceived Risk

Perceived risk is defined as a consumer's perceptions of the uncertainty and the possible undesirable consequences of buying a product or service [42]. It's only human. People make mistakes, learn from them, and move on to the next challenge usually without dire consequences. But in business, particularly in information technology, mistakes can be costly. From information theft to lost worker productivity to missed sales opportunities, technology errors can put your business at risk. [43]

Legal risk becomes an important issue in internet banking, and one aspect of this is how any losses from security breaches should be apportioned between banks and their customers. Customers should be responsible for any security breach or system problem that is due to negligence on their part, and this should be reflected in the contractual agreements for internet banking services. But if the damage is occurred for system breakdown, negligence of bank employees, attack by hacker or any other parties; the bank must be liable to cover the damage [44] this also results in large security risks imposed on users that have little or no knowledge about the risks and damage that can be inflicted by using the Internet.[45] In history of IT especially security incidents, the biggest mistake has always been to rely on the trust of the other systems and assume the systems are not compromised.

H3 a: the Perceived risks have a negative impact on perceived usefulness.

H3 b: the Perceived risks have a negative impact on Security and privacy

As Koller (1988) wrote, the level of the significance of a decision specifies the influence of the potential risk. It is obvious that the acceptance of electronic trading is a long-term important decision for most of the customers and that is the reason why the role of risking is so important here [46]. Lim also indicated that the perceived risks are so important in explaining the customers' behavior, in that, the customers are willing to increase their satisfaction from on-line purchase to its maximum rate by stopping making mistakes. Regarding the theory of the perceived risk, the customers perceive the risk because they face a kind of uncertainty and potential dissatisfaction. Such feelings originate from the consequents of their purchase [47] the risk perception of thee. Banking customers primarily grows out of the IT lapses and the resultant losses incurred in fraudulent access to customer accounts [48] the main components of Perceived Risk are perceived security and trust, which have emerged as the top issues in banking adoption. This construct reflects an individual's subjective belief about the possible negative consequences of some type of planned Action, due to inherent uncertainty which is likely to negatively influence usage intentions. Trust is at the heart of all kinds of relationships [49] there are still customers who fear to make use of IB, as they are concerned with security aspects of such a system. Previous research has found the risk associated with possible losses from the online banking transaction is greater than in traditional environments [50]

5.4 Security and privacy

Security Privacy is an indicator used to measure the perceived security and privacy of e-banking [51]. It consists of five elements namely the financial security of e-banking, the trust which individuals have in the service, privacy protection of the customer, security level password and the presence of a third party to validate the Bank's identity. Ease of Use is also an index based on Davis (1989), which contains 4 elements namely e-banking is easy to use, simple, has a user-friendly website and is a flexible system for interaction [52].

Concept of perceived security may be useful to capture the user's subjective perception of the security risks involved in e-banking. Several studies including Jih et al. (2005) indicate that user adoption of e-banking is affected by perceived security. This supports a view of security as crucial to the overall usability of e-banking systems [53] Security issues are a major source of concern for everyone both inside and outside the banking industry. E-banking increases security risks, potentially exposing hitherto isolated systems to open and risky environments [54] the importance of security and privacy for the acceptance of online banking has been noted in many banking Studies [55]

H4. Security and privacy have a negative impact on trust

If the index of security and privacy is low, it generates fears among customers leading to reduced customer Trust indicator; in this case the customer will go to non-use of electronic banking

5.5 Trust

Trust can be defined as "function of the degree of risk involved in the e-banking transaction ,and the outcome of trust is proposed to be reduced perceived risk ,leading to positive intention towards adoption of e -banking [56].Trust and security have always been essential features of the banking system and protection of information assets is necessary to establish and maintain trust between the bank and its customers [57] Lack of Customer trust is a major hurdle in the growth of e-banking although winning consumer trust is more important in online environment; online trust does share a number of characteristics with the offline trust [58] Customer trust in the technology of e-banking is a huge hurdle given the intangible nature of the service .trust includes essential notions of technology security Reliability and protection against hackers and theft of client identity or financial information [59] added that to increase external validity of TAM, it is necessary to further explore the nature and specific influences of technological and usage–context factors that may alter the user's acceptance. For instance, recent research has indicated that "trust" has a striking influence on users' willingness to engage in online exchanges of money and sensitive personal information [60] The use of this new technology is too new to the developing countries, and this may be a cause of the lack of trust from the customers in using the internet banking or e-banking as a whole. When the customers have a feeling of no trust and uncertainty for the phenomena, it is believed that they look at it as a risk [61] numerous studies have tried to find correlations between trust and experience with a new system, concept, or relationships, including a correlation to the frequency of e-commerce Activity, and as such, other researchers have noted that trust may be significantly influenced by the culture of a given society [62] the importance of trust and security as direct or indirect influencing factors in an individual's intention to engage in online transactions. Trust refers to a degree of an individual willingness to be vulnerable to the actions of others [63].

H5. Lack of Trust has a negative impact on actual e-banking Use

6. CONCLUSION AND FUTURE WORK

Through this study we conclude that the level of customer knowledge in information technology is important factor influencing the security of banking, in other words the higher the level of customer knowledge in information technology the fewer security flaws that may occur, and this is an indicator that the banking security risks will be reduced and increase the degree of safety , this shows that increase the degree of safety generate confidence among customers who use banking applications through the Internet, We conclude that the high level of customers knowledge leads the customers to take precautions and follow the correct behavior to protect their data from attack. When users become more familiar with a technology and Internet, in this case, they tend to have higher expectations towards the technology. This research is initial step for future work; in the future we will conduct experimental studies to test our model.

7. REFERENCES

[1] Mahdi, S. and Mehrdad, A. E-Banking in Emerging Economy: Empirical Evidence of Iran, International Journal of Economics and Finance, Vol. 2, No. 1, February 2010, pp. 201-209.

[2] Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. International Journal of Bank Marketing, Vol. 17 No. 7, pp. 324-34.

[3] Hertzum, M., Juul, .N.C., Jorgensen N., Usable Security and E-Banking: ease of use vis-a-vis security, Australasian Journal of Information Systems, Vol 11, No 2 (2004).

[4] Rahmath Safeena, Hema Date and Abdullah Kammani , Internet Banking Adoption in an Emerging Economy: Indian Consumer's Perspective , International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011.

[5] http://www.buzzle.com/articles/internet-banking-problems.html.

[6] Akhlaq, Mohammed ather and Shah, Asadullah (2011) Internet banking in Pakistan: finding complexities. Journal of Internet Banking and Commerce, 16 (1). pp. 1-14.

[7] Davis, F.D, A technology acceptance model for empirically testing new end-user information systems: Theory and results, Doctoral Dissertation, Sloan School of Management, Massachusetts Institute of Technology, 1986.

[8] Tan, M. and Teo, T. (2000) Factors Influencing the Adoption of Internet Banking, Journal of the Association for Information Systems, 1, 5, 1-42.

[9] Davis, F 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly. Vol. 13 No. 3, pp 319 –340.

[10] http://socialreport.msd.govt.nz/documents/knowledge-skills-social-report-2010.pdf.

[11] Lassar, W.M., Manolis, C. and Lassar, S.S., (2005). The relationship between consumer innovativeness, personal characteristics, and online banking adoption. International Journal of Bank Marketing, 23 (2), pp 176-199.

[12] Ongkasuwan M, Tantichattanon W (2002). A Comparative Study of Internet Banking in Thailand. Retrieved on [May, 2010] from World Wide Web: http://www.ecommerce.or.th/nceb2002/paper/55- A_Comparative_Study.pdf.

[13] http://www.ukessays.com/essays/information-systems/information-security- crime-management.php.

[14] http://www.anz.com/personal/ways-bank/security/online-security/threats-banking-safety/computer-threats/.

[15] Jason Milletary, Technical Trends in Phishing Attacks, CERT Coordination Center1, (2005), pp. 1-17.

[16] Williamson, Gregory D. Enhanced Authentication In Online Banking, Journal of Economic Crime Management, Vol. 4, Issue 2, 2006.

[17] New Perspectives on Computer Concepts 2013: Introductory, June Jamrich Parsons, Dan Oja – 2012.

[18] Internet GIS: Distributed Geographic Information Services for the Internet. Zhong-Ren Peng, Ming-Hsiang Tsou - 2003 - 679 :عدد الصفحات

[19] HTTP: Developer's Handbook ,Chris Shiflett – 2003.

[20] S. Kierkegaard, "Swallowing the bait, hook, line and sinker: Phishing, pharming and now ratting!," in Managing Information Services in Financial Services H. R. Rao, M. Gupta, and S. J. Upadhyaya, Eds. USA: IGI Publishing, 2008, pp. 241-253.

[21] Auburn University, http://www.auburn.edu/oit/phishing/

[22] Gerald Goh Guan Gan, Tan Nya Ling, Goh Choon Yih and Uchenna Cyril Eze; Phishing: A Growing Challenge for Internet Banking Providers in Malaysia Communications of the IBIMA Volume 5, 2008 133 Phishing: A Growing Challenge for Internet.

[23] R. Dhanalakshmi, C. Prabhu, C. Chellapan , Detection Of Phishing Websites And Secure Transactions , International Journal of Communication Network and Security(IJCNS-2011), Volume. 1 Issue. 2.

[24] http://educationinfree.wordpress.com/2012/05/31/what-is-keylogger-2/.

[25] http://www.iwar.org.uk/comsec/resources/spyware/thompson.htm#_ftnref6.

[26] http://www.antivirusworld.com/articles/keylogger.php.

[27] Adrian McCullagh, William Caelli ,Who Goes There? Internet Banking: A Matter of Risk and Reward, Information Security and Privacy - ACISP 2005, 4-6 July 2005, Australia, Queensland, Brisbane.

[28] For detailed information on PWSteal.Bankash.A (MCID 4326), see http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bankash.a.html.

[29] French, T. K. Liu, K. and Springett, M. , 'A Card-Sorting probe of E-Banking Trust Perceptions', Proceedings HCI 2007, BCS, (2007) ISBN 1-902505-94-8.

[30] Juliet Bugembe , Perceived Usefulness, Perceived Ease Of Use, Attitude and Actual Usage Of A New Financial Management System: A Case Study Of Uganda National Examinations Board, JUNE 2010.

[31] Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. Information & Management, 40, 191–204.

[32] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of Information technology. MIS Quarterly, 13(3), 319-340. http://www.jstor.org/pss/249008.

[33] Wadie Nasri, Factors Influencing the Adoption of Internet Banking in Tunisia, International Journal of Business and Management, Vol. 6, No. 8; August 2011.

[34] syed shan e raza, impact of user it and internet skills on online banking, Input to innovative banking strategies, international journal of social sciences and humanity studies Vol 3, no 1, 2011 issn: 1309-8063 (online).

[35] Sam Ian , Online Banking and the role of CRM: The impact of the internet as online business platform on CRM (Study of Online banking in the UK).

[36] Muhammad Muazzam Mughal, Muhammad Farhan, Kamran Ali, Abdul Jabbar Khan, Accepting of E-banking among Banking Customers of Pakistan, Information Management and Business Review Vol. 4, No. 6, pp. 332-339, June 2012.

[37] Raphaël K. Akamavi, (2005) "Re-engineering service quality process mapping: e-banking process", International Journal of Bank Marketing, Vol. 23 Iss: 1, pp.28 – 53.

[38] Henny Medyawati 1, Marieta Christiyanti 2 and Muhammad Yunanto, e-banking adoption analysis using technology acceptance model (tam): empirical study of bank customers in bekasi city , 2011 International Conference on Innovation, Management and Service IPEDR vol.14(2011).

[39] Fred D. Davis , Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly, Vol. 13, No. 3 (Sep., 1989), pp. 319-340.

[40] Geetha Kallamarthodi, Malarvizhi Vaithiyanathan; Empirical Assessment of a Modified Technology Acceptance Model in Emerging Economy: An Assessment from the Perspective of Indian Consumers", 2011 International Conference on E-business, Management and Economics IPEDR Vol.25.

[41] Apostolos Giovanis, Spiridon Binioris; factors affecting internet banking usage behavior: an empirical investigation of Greek customers, Proceedings of the 2nd International Conference: Quantitative and Qualitative Methodologies in the Economic and Administrative Sciences.

[42] Littler, D., Melanthiou, D. (2006) ‘Consumer perceptions of risk and uncertainty and the implications for behavior towards innovative retail services: the case of internet banking’, Journal of Retailing and Consumer Services, 13, 431-43.

[43] Intel Top 10 Technology Risks http://www.nor-tech.com/solutions/dox/Top_10_Technology_Risks.pdf.

[44] Khan, A.R. and Karim, M. (2010). E-Banking and extended risks: How to deal with the challenge, Paper Presented to the Department of Finance and Banking, Rajshahi University, pp.17.

[45] André L.M. dos Santos, Richard A. Kemmerer, Safe Areas of Computation for Secure Computing with Insecure Applications, 15th Annual Computer Security Applications Conference (ACSAC '99).

[46] Koller M (1988). Risk as a determinant of trust. Basic Appl. Soc.Psychol., 9(4): 265–276.

[47] Lim N (2003). Consumers'' perceived risk: sources versus consequences. Electron. Commer. Res. Appl., 2: 216–228.

[48] Littler, Dale and Melanthiou, Demetris (2006), “Consumer Perceptions of Risk and Uncertainty and The Implications for Behavior towards Innovative Retail Services: The Case Of Internet Banking, Journal of Retailing and Consumer Revices, Vol: 13:431-443.

[49] AL. Zhao, NK. Lewis, SH. Lloyd, and P. Ward, (2010), “Adoption of internet banking services in China: is it all about trust?” International Journal of Bank Marketing, vol. 28, no. 1, pp. 7-26.

[50] L. Bradley and K. Stewart, “Delphi study of Internet banking,” Marketing intelligence and planning, vol. 21, no. 5, pp. 272-281,2003.

[51] Taylor, S. and Todd, P.A. (1995). Understanding information technology usage: a test of competing models. Information Systems Research, 6(2), 144-176.

[52] Tandrayen-Ragoobur, Verena; Ayrga, Anisha, Is Mauritius Ready to E-Bank? From A Customer and Banking Perspective, SOURCE Journal of Internet Banking & Commerce; Apr2011, Vol. 16 Issue 1.

[53] Morten Hertzum, Niels Jorgensen, Mie Norgaard: Usable Security and E-Banking: ease of use vis-a-vis security. Australasian J. of Inf. Systems 11(2) (2004).

[54] Carol Sergeant, Director, Banks & Buildings Societies, Financial Services Authority, http://www.fsa.gov.uk/library/communication/speeches/2000/sp46.shtml.

[55] Sathye, M. (1999), "Adoption of Internet banking by Australian consumers: an empirical investigation", International Journal of Bank Marketing, Vol. 17 No. 7, pp. 324-34.

[56] Hamid Reza Peikari ,A Study on the Interrelations between the Security-Related Antecedents of Customers’ Online Trust, Global Communications in Computer and Information Science Volume 92, 2010, pp 139-148.

[57] Jayaram Kondabagil , Risk Management in Electronic Banking: Concepts and Best Practices, Ch7, P-69- 2007.

[58] Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. Computers in Human Behavior, 21.

[59] Jennifer Isern,A cross-country analysis of the effects of e-banking and financial, Nova Southeastern University – 2008.

[60] Hoffman, DL, Novak, TP & Peralta, M 1999, 'Building consumer trust online', Communications of the ACM, vol. 42, no. 4, pp. 80-85.

[61] Reza Shafei , Vala Mirani, Designing a model for analyzing the effect of risks on e-banking adoption by customers: A focus on developing countries, African Journal of Business Management Vol. 5(16), pp. 6684-6697, 18 August, 2011.

[62] McKnight, D. and N. Chervany. (2001). "What trust means in e-commerce customerrelationships: An interdisciplinary conceptual typology." International Journal of Electronic Commerce 6: 35-59.

[63] Mayer, R. C., Davis, J. H. & Schoorman, F. D.(1995). 'An Integrative Model of Organizational Trust,' Academy of Management Review, 20(3):709-734.

INSTRUCTIONS TO CONTRIBUTORS

The *International Journal of Computer Science and Security (IJCSS)* is a refereed online journal which is a forum for publication of current research in computer science and computer security technologies. It considers any material dealing primarily with the technological aspects of computer science and computer security. The journal is targeted to be read by academics, scholars, advanced students, practitioners, and those seeking an update on current experience and future prospects in relation to all aspects computer science in general but specific to computer security themes. Subjects covered include: access control, computer security, cryptography, communications and data security, databases, electronic commerce, multimedia, bioinformatics, signal processing and image processing etc.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Started with Volume 7, 2013, IJCSS is appearing in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCSS LIST OF TOPICS

The realm of International Journal of Computer Science and Security (IJCSS) extends, but not limited, to the following:

- Authentication and authorization models
- Computer Engineering
- Computer Networks
- Cryptography
- Databases
- Image processing
- Operating systems
- Programming languages
- Signal processing
- Theory
- Communications and data security
- Bioinformatics
- Computer graphics
- Computer security
- Data mining
- Electronic commerce
- Object Orientation
- Parallel and distributed processing
- Robotics
- Software engineering

CALL FOR PAPERS

Volume: 7 - **Issue:** 5

i. Submission Deadline : October 30, 2013 **ii. Author Notification:** December 01, 2013

iii. Issue Publication: December 31, 2013

CONTACT INFORMATION

Computer Science Journals Sdn BhD
B-5-8 Plaza Mont Kiara, Mont Kiara
50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6207 1607
006 03 2782 6991

Fax: 006 03 6207 1697

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2013
COMPUTER SCIENCE JOURNALS SDN BHD
B-5-8 PLAZA MONT KIARA
MONT KIARA
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6207 1607
006 03 2782 6991

FAX: 006 03 6207 1697
EMAIL: cscpress@cscjournals.org