International Journal of Computer

(IJC)

ISSN 2307-4523 (Print & Online)

© ***Global Society of Scientific Research and Researchers***

http://ijcjournal.org/

Security Enhancement System Based on the Integration of Cryptography and Steganography

Zin May Zaw[a]*, Su Wai Phyo[b]

[a,b] *Department of Information Technology, Mandalay Technological University*
The Republic of the Union of Myanmar
[a] *Email:zinmay83@gmail.com*
[b] *Email:swp2006@gmail.com*

Abstract

Nowadays, due to the widespread use of data exchange in electronic way, the information security has become important in data storage and transmission. Lack of security makes many problems in security awareness applications. The two kinds of information that are widely used in daily communication are image and text. Steganography and cryptography are both ways to protect the data security against various attacks. Thus, this work focuses on the enhancement of not only image but also information security based on the combination of cryptography and steganography methods. From the cryptography point of view, image security is enhanced based on the combination of proposed block-based transformation and encryption technique. Firstly, the original image is transformed with proposed block-based transformation algorithm to obtain better robustness of image encryption. And then, the generated transformed image is encrypted by using Blowfish encryption algorithm. After getting the encrypted image, a steganography approach provides the data hiding system by using this encrypted image as a cover for information security. Moreover, to prove the advantages of using combination process (proposed transformation and Blowfish encryption) rather than single encryption, performance comparison is made by calculating the correlation and entropy of encrypted images generated by combination process and Blowfish encryption algorithm.

Keywords: block-based transformation; Blowfish; LSB; correlation; entropy.

1. Introduction

With the rapid growth of internet usage in today's communication system, data security has become a fundamental issue.

----

* Corresponding author

Steganography and cryptography are two popular ways of sending the information in a secret way. One hides the existence of the message and the other distorts the message itself. This research paper mainly focuses on to develop a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like cryptography and steganography. The main advantage of the system is that it encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable.

Today, most of the processes in government, military communication, financial institution, medical imaging and private business greatly deal with data that are in the form of image. Therefore, the security of digital images has become important and attracted much attention. Encryption is the preferred technique for protecting the security of image data. But, in general, most of the cryptographic encryption algorithms are used for text data. Although, the traditional encryption algorithms can be used to encrypt the images directly, it may not be suitable for some specific characteristics of image such as large data size and high correlation among pixels [1,2]. In the original image, the neighboring pixels in the image are strongly correlated. Due to the high correlation among pixel elements, the attacker can easily predict the value of any given pixels from the value of its neighbors [3,4]. This problem can be solved by decreasing the correlation among pixel elements by using certain transformation technique. But, according to many research areas, neither of transformation and encryption technologies alone is secure against various attacks [5]. Therefore, in this system, a block-based image transformation algorithm is proposed as pre-encryption step and then the combination of image transformation and Blowfish encryption technique is effectively used to enhance image security. Correlation and entropy are also calculated to measure the security level of encrypted images generated by combination process and Blowfish encryption.

In the other word, steganography is the best way of hiding the secret message in innocuous media (carriers) such as text, image, audio, video and protocol without changing the perceptual quality of data. Among these different carriers, digital image is the most popular cover object because large amount of redundant bits are presented in the digital representation of an image. Moreover, Least Significant Bit (LSB) insertion is very popular and simple technique for embedding information into cover image. Therefore, in order to further strengthen the cryptography technique of proposed work, a steganography approach for data hiding is also added by using LSB embedding technique. In this system, the encrypted cover image is used as cover object for the image steganography. By using encrypted cover image, the attacker cannot know that whether or not secret message is present within encrypted image and they will notice to attack only the encrypted image. So, it can get high security for hidden message.

The rest of the paper is organized as follow: literature review is presented in section two. Background theory is described in section three. Section four presents the design of the proposed system. Then, system implementation and experimental results are shown in section five. Finally, section six draws the conclusion.

2. Literature Review

With the large flood of information and the development of the digital format, it becomes the necessary to find appropriate protection for information.

Encryption is a common technique to uphold the image security. Moreover, information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography [6]. Therefore, new proposed algorithms to enhance the security requirements are developed in order to get efficient reliability in many research areas. In reference [7], Dr. S. Kishore Reddy proposed encrypted data hiding system in encrypted cover images. In this system, the author used three encryption methods such as RSA, reversible data hiding method and cat map transform to encrypt the image and then secret information is embedded within the encrypted image by using LSB embedding technique. Moreover, the performance comparison is made between these three methods in term of Peak Signal to Noise Ratio (PSNR) values. The main objective of the author is to enhance both image and data security by studying the various encryption schemes. Then, Vinay pandey [8] proposed a new method that combines image cryptography, data hiding and steganography technique for denoised and safe image transmission purpose. In this method, the original image is encrypted with stream cipher algorithm and the secret message (patient information) is embedded using lossless data embedding technique with data hiding key for more security. Moreover, S. Vasumathi Kannaki [9] proposed a secure data hiding system based on the integration of cryptography and steganography techniques. In this work, the secret message is firstly encrypted with AES algorithm. And then, the encrypted message is hidden in transformed image which are generated by using Discrete Cosine Transformation (DCT). To obtain better security, the author hides one part of encrypted message in DCT of an image and the remaining part of the secret message is used to generate two secret keys.

According to the literature and concepts of security enhancement approaches which are pointed out from the previous researches, the main aim of this work is to propose a security enhancement system based on the combination of cryptography and steganography.

3. Background Theory

The two main theories used to enhance image security are Blowfish encryption algorithm and proposed block-based transformation algorithm. For data security, the LSB embedding method is used to hide secret message within cover image. Moreover, for performance analysis and security consideration of image encryption approach, entropy and correlation are also calculated in this system.

3.1 Proposed Block based Transformation Algorithm

In order to enhance the image security, this work proposes a block-based image transformation algorithm to combine with blowfish encryption. The purpose of using transformation process as pre-encryption step is to reduce high correlation among pixel elements as low as possible. Transformation is the process of dividing the original image into random number blocks which are shuffled and placed randomly within the image to build a newly transformed image. Proposed transformation algorithm is as follows: the original image is divided into n x n number of pixel blocks which one contains specific number of pixels. Then, these blocks are transformed into new location within image by using random function. If the random function generates the same number of block that has been selected once, the new number block is generated to avoid the overlapping of blocks within the transformed image. In this process, the secret key is used to determine the seed.

The seed plays a main role in building the transformation table which is then used to generate the transformed image. After getting the transformation table, it is also permuted by using columnar transposition cipher algorithm to obtain better security. In the columnar transposition cipher process, the input key must be the character and key length must be equal to the column numbers of block sizes. Then, the order of keys is calculated and the numbers of columns are rearranged according to the order of key. Because of using double transformation, it becomes difficult to predict the value of any given pixel from the values of its neighbors and can enhance image security. Moreover, for obtaining better image security, the divided block size should be small because fewer pixels keep their neighbors.

Algorithm: Creating the Transformation Table.

Input: Bmp Image File, key

Output: Transformation Table

```
(1)     Load image
(2)     Input Key
(3)     Get image width and high
(4)     Divide image into n x n pixel blocks
(5)     Calculate horizontal pixel blocks = Int (Image width/n)

Calculate vertical pixel blocks = Int (Image high/n)

(6)     Calculate the number of pixel blocks = Horizontal pixel blocks x Vertical pixel blocks
(7)     Seed = Hash value (key)
(8)     Randomize ()
(9)     I = 0, Count=0

While I < Number of pixel blocks

R= random number between 0 and number of blocks -1

While R is selected block and Count < 500

R = random number between 0 and number of blocks -1

If R is selected block number then

Count = Count+1

Else

Count = 0
```

```
End if

End while

I ← R

I + = 1

End while
```

Algorithm: Columnar Transposition Cipher

Input: Transformation Table, String Key

Output: Permuted Image Block Table

(1) Load transformation table
(2) Input key (Key size must be the same as the column numbers of block size)
(3) Calculate the order of key
(4) Rearrange the image blocks along with column using the index number of key
(5) Output permuted image block table

3.2 Blowfish Encryption

Blowfish is a symmetric encryption algorithm that can be used as a drop in replacement for DES or IDEA. It was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms [10]. It is a symmetric block cipher which means that it divides the message into blocks of fixed length during encryption or decryption. It encrypts 64-bit block of plaintext as input and produces corresponding 64-bit block of ciphertext as output. It takes variable length key, ranging from 32 bits to 448 bits. Its structure is based on 16 round Feistel network. Block diagram of Blowfish encryption process is shown in Figure 1.

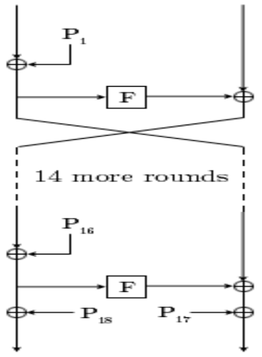


Figure 1: Block Diagram of Blowfish Encryption

This algorithm consists of two parts: *Key expansion part:* In Key expansion part, a key of at most 448 bits is being converted into several subkey arrays, totaling 4168 bytes. *Data encryption part:* In Data encryption part, 16-round Feistel network is used. Each round consists of key dependent permutation and key and data dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [11]. The encryption process works as follow: The input is 64-bit data element, X. Divide X into two 32-bit halves: X_L, X_R. Then,

for i = 1 to 16:

$X_L = X_L$ XOR P_i

$X_R = F(X_L)$ XOR X_R

Swap X_L and X_R

After the sixteenth round, swap X_L and X_R again to undo the last swap. Then,

$X_R = X_R$ XOR P_{17} and

$X_L = X_L$ XOR P_{18}

Finally, recombine X_L and X_R to get the ciphertext. F-function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output. Since Blowfish is a Feistel network, it can be inverted simply by XORing P_{17} and P_{18} to the ciphertext block. The block diagram of function F is shown in Figure 2. Decryption process is similar to encryption except that in decryption, the P-entries, P_1, P_2,…, P_{18} are used in reverse order.

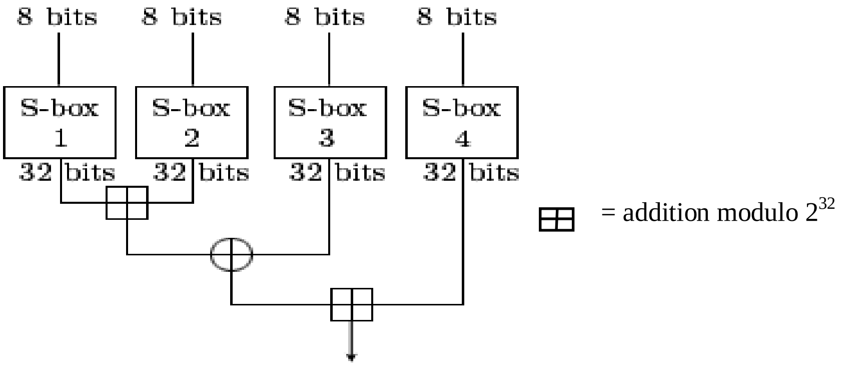


Figure 2: Block Diagram of Function F

3.3 Least Significant Bit (LSB)Insertion

One of the most common techniques used in steganography today is the least significant bit (LSB) insertion method [12].

In this method, the least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Firstly, the image data and secret message are accessed as a series of bits. Then, the bits of the secret message are inserted into the LSB of the bytes of the encrypted cover image. When using a 24-bit image, a bit of each of the red, green and blue color components can be used since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800x600 pixel image can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [13]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)

(1010011**0** 1100010**1** 0000110**0**)

(1101001**0** 1010110**0** 0110001**1**)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [13].

3.4 Entropy and Correlation

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon [14]. Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy H(*m*) of a message source can be measured by equation (1).

$$H(m) = -\sum_{i=0}^{m-1} p(m_i)\log_2 p(m_i) \tag{1}$$

where m is the total number of symbols, $m_i \in m$ and p(m_i) represents the probability of occurrence of each symbol m_i. Logarithm of base 2 denotes that the entropy is expressed in bits.

Correlation is a statistical measure of image security that expresses a degree of relationship between two adjacent pixels in an image. In most of the natural images, the values of neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors).

The aim of correlation measure is to keep the amount of redundant information available in the encrypted image as low as possible [15]. It is calculated by using equation (2).

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{(n\sum(x^2) - (\sum x)^2)(n\sum(y^2) - (\sum y)^2)}} \tag{2}$$

where

r = correlation value

n = number of pairs of adjacent pixels randomly selected from image

x and *y* = the intensity values of two neighboring pixels in image

4. Proposed System Architecture

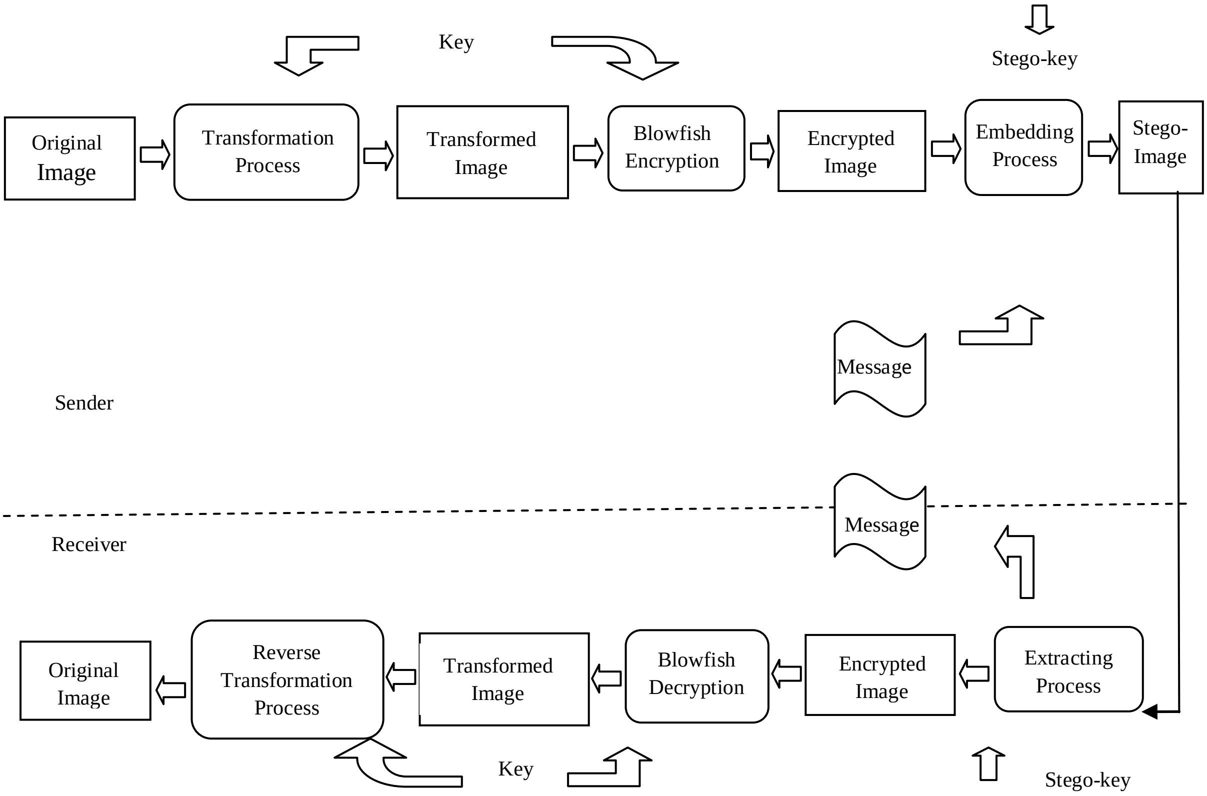


Figure 3: General Block Diagram of Information Hiding Process Using Encrypted Cover

At the sender side, the original image is firstly transformed with proposed block-based image transformation algorithm to obtain better robustness of image encryption. And then, the generated transformed image is encrypted with Blowfish encryption. It is expected to enhance the security level of encrypted image by using the combination process (transformation and Blowfish encryption) rather than single encryption process.

After getting the encrypted image, steganography approach is also applied for hiding the secret information within it before transmitting to the receiver side. At the receiver side, the original image can be retrieved by using extracting process, image decryption and reverse transformation process.

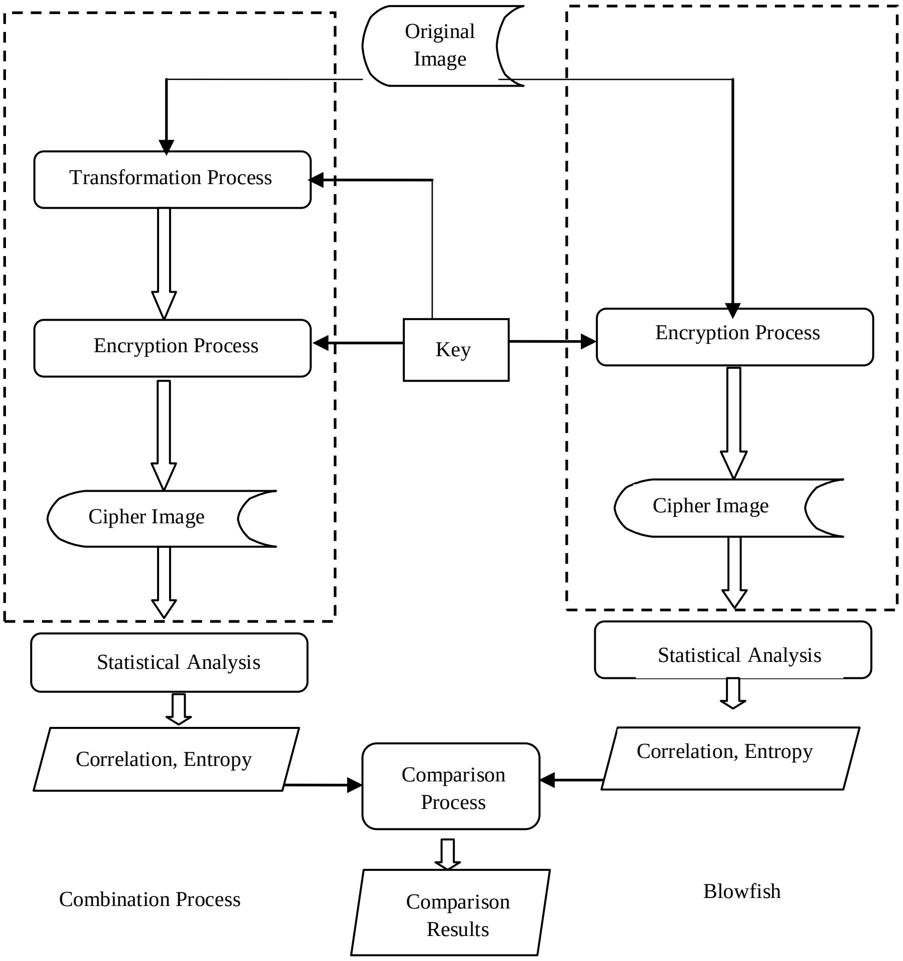


Figure 4: Block Diagram of Performance Comparison Process

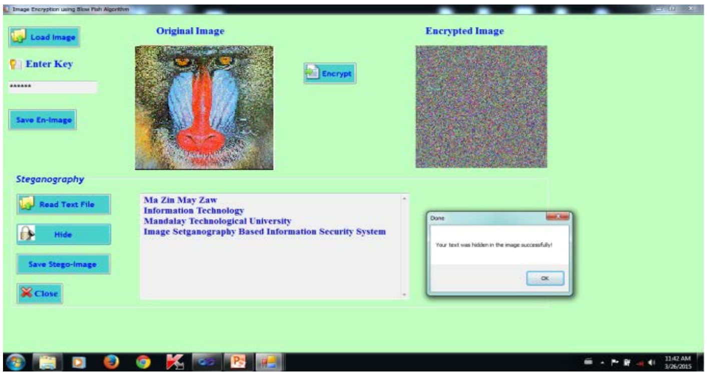
After that, for performance consideration, the entropy and correlation are calculated to show the advantages of using combination process (proposed transformation and blowfish encryption) in image encryption rather than Blowfish. The block diagram of performance comparison is illustrated in Figure 4. The result shows that the encrypted image using combination process has lower correlation and higher entropy values rather than single encryption process.

5. Implementation Results

This section shows the implementation results of the proposed work which is implemented by using C# programming language. The first part is a series of interfaces of security enhancement system and the second part is performance evaluation.

5.1 Graphical User Interface of Security Enhancement System

For this security enhancement system, there are two main processes for image encryption: “Blowfish Encryption” and “Proposed Combination Process”. If the user selects “Blowfish Encryption” process, the original image is encrypted with Blowfish by using “Encrypt” button. After getting the encrypted image, the secret message is loaded by using “Read Text File” button and hides it within encrypted image using “Hide” button. Then, the generated stego-image is saved by using “Save Stego-Image” button as shown in Figure 5. In decryption process, the stego-image which is saved is reloaded and the hidden message is firstly extracted. After that, the original image can be obtained by using Blowfish decryption.



Ma Zin May Zaw
Information Technology
Mandalay Technological University
Image Setganography Based Information Security System

Your text was hidden in the image successfully!

Figure 5: Blowfish Encryption and Data Hiding

On the other hand, if the “Proposed Combination Process” is selected, the original image is firstly needed to transform by using proposed block-based image transformation algorithm as illustrated in Figure 6.

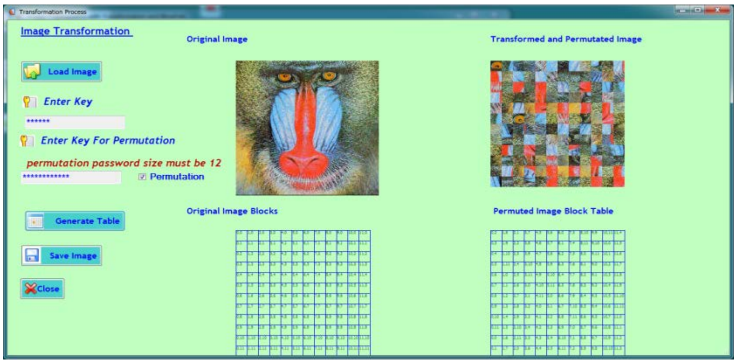
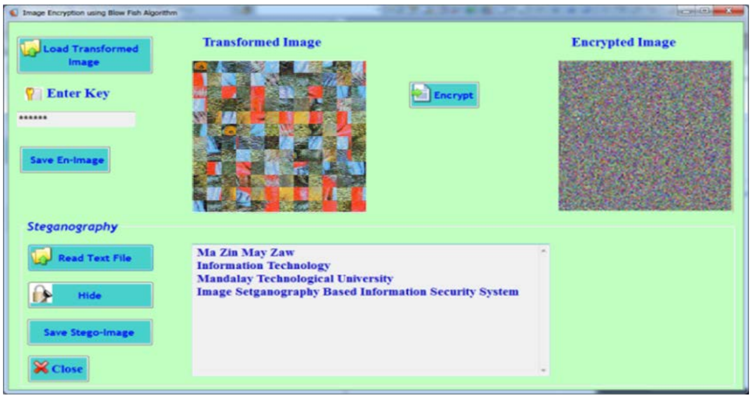


Figure 6: Transformation Process

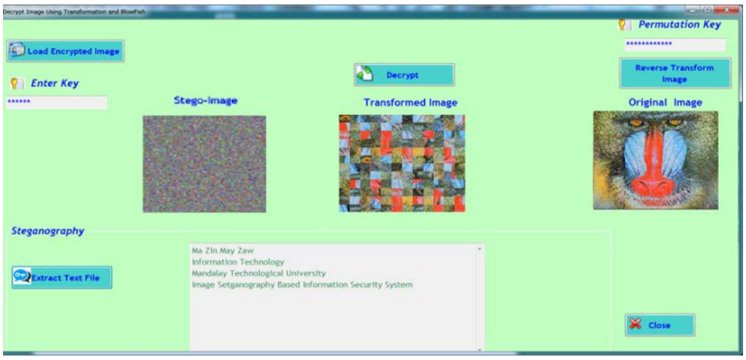
In the transformation process, the original image is loaded and the key is inserted. Key is the main role in creating transformation table. And then, the transformation table is also permuted by the columnar transformation cipher algorithm for better security. Then the generated transformed image is saved. After getting the transformed image, it is encrypted by using Blowfish algorithm as shown in Figure 7. Then, the secret message is hidden within encrypted image by using “Hide” button and the generated stego-image is saved.



Ma Zin May Zaw
Information Technology
Mandalay Technological University
Image Setganography Based Information Security System

Figure 7: Encryption and Data Hiding Using Combination Process

Finally, at the receiver side, the stego-image is reloaded and firstly extracts the secret information. After that, the original image can be retrieved by using “Decrypt” and “Reverse Transformation” buttons as illustrated in Figure8.



Ma Zin May Zaw
Information Technology
Mandalay Technological University
Image Setganography Based Information Security System

Figure 8: Extracting ,Decryption and Reverse Transformation Using Combination Process

5.2 Performance Evaluation

In this part, the entropy and correlation are used to measure and compare the security level of four images such as original image, transformed image, encrypted image generated by combination process and encrypted image generated by Blowfish algorithm alone. It is expected that the encrypted image generated by combination process has lower correlation and higher entropy value than the other images. Moreover, in order to evaluate the impact of the number of block size on correlation and entropy value, the image is tested by dividing three different number of block sizes such as 30x30 pixel blocks, 20x20 pixel blocks and 10x10 pixel blocks in this system. Figure 9 shows the original bmp image, the size of 256x256 pixels with 256 color and its encrypted images.

The experimental results of entropy and correlation for three different block sizes are shown in Table1 and the graphical representations of these values are shown in Figure 10 and 11. According to the experimental results, the encrypted image using combination process has lower correlation and higher entropy value than all of the other images.

Moreover, it can be clearly seen that the smaller the block size, the better the security of image.

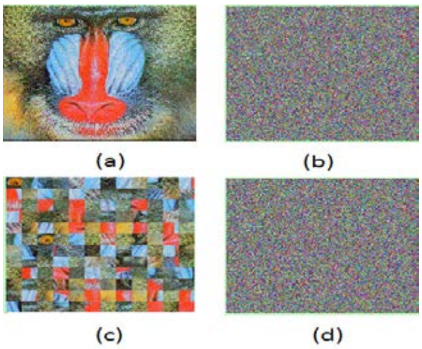


Figure 9: (a) Original Image (b) Encrypted Image Using Blowfish (c) Encrypted Image Using Transformation Algorithm (d) Encrypted Image Using Combination of Transformation and Blowfish Encryption

Table 1: Analytical Results of Entropy and Correlation

Image	30x30 pixels		20x20 pixels		10x10 pixels	
	Entropy	Correlation	Entropy	Correlation	Entropy	Correlation
Original Image	7.682	0.9341	7.682	0.9341	7.682	0.9341
Transformed Image	7.71	0.725	7.7141	0.6635	7.7226	0.5981
Encrypted Image Using Single Blowfish	7.9266	0.0659	7.9266	0.0659	7.9266	0.0659
Encrypted Image Using Combination Process	7.981	0.0532	7.9902	0.0486	7.9999	0.0379

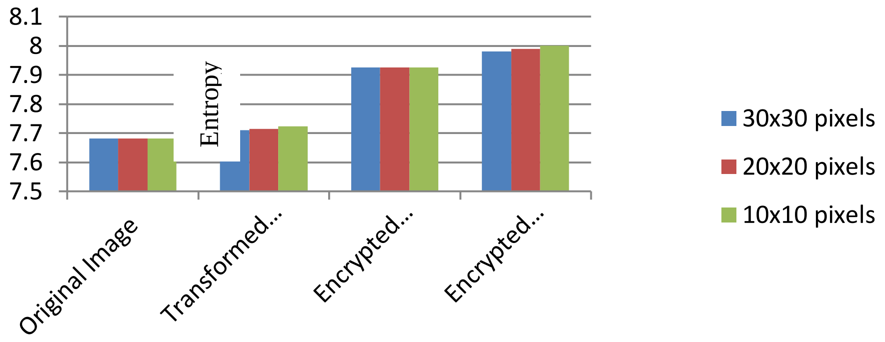


Figure 10: Entropy Analysis for Three Different Block Sizes: 30x30 pixels, 20x20 pixels and 10x10 pixels

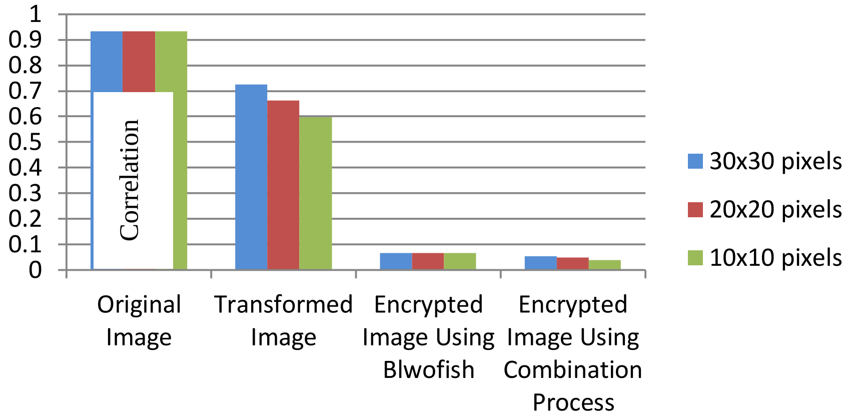


Figure 11: Correlation Analysis for Three Different Block Sizes: 30x30 pixels, 20x20 pixels and 10x10 pixels

6. Conclusion

This paper proposes a security enhancement system for image and text which are widely used over electronic communication. At cryptographic point of view, the combining usage of image transformation and encryption technique makes the attackers more difficult for decryption process. Moreover, it can be clearly seen that there are lower correlation and higher entropy value when the proposed transformation algorithm is applied as pre-encryption step according to the analytical results. On the other hand, at the steganography point of view, the attackers cannot be easily suspicious the existence of hidden information as the encrypted cover is used for hiding the secret message. Thus, it can achieve the security requirements such as confidentiality of hidden message. Therefore, the proposed system can be applied in many security awareness application areas. In this system, only two image file types such as jpeg and bmp can be used for image cover. As further extension, the proposed block-based transformation algorithm can be tested together with other cryptographic encryption algorithms.

References

[1] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. *Proceedings of Advanced Concepts for Intelligent Vision Systems*,2002.

[2] S.Fong, P.B. Ray, and S. Singh, "Improving the lightweight video encryption algorithm," *proceeding of iasted international conference, single* processing, pattern recognition and application, 2002, pp. 25-28.

[3] S. P. Nana'vati., P. K. panigrahi. "Wavelets:applications to image compression- I," *joined of the scientific and engineering computing*, vol. 9, no . 3, 2004, pp. 4-10.

[4] AL. Vitali, A. Borneo, M. Fumagalli and R. Rinaldo, "Video over IP using standard-compatible multiple description coding," *Journal of Zhejiang University- Science A*, vol. 7, no. 5 ,2006, pp. 668-676.

[5] Li. Shujun, Li.Chengqing and C. Guanrong, “A general cryptanalysis of permutation-only multimedia encryption algorithms”, *Fellow, IEEE*. Available: http://eprint.iacr.org / 2004.

[6] Isbell R. A.: "Steganography: Hidden Menace or Hidden Saviour", Steganography White Paper, 10th May, (2002).

[7] Dr.S.Kishore Reddy, "Encrypted data hiding in encrypted images", *International Journal of Research in Engineering and Applied Sciences*, vol.2, pp. 50-59, September 2012. Available: http://www.euroasiapub.org.

[8] Vinay Pandey, "Medical image protection using cryptography, data hiding and steganography", *International Journal of Emerging Technology and Advanced Engineering,* vol.2. pp. 106-109, January 2012. Available: http://ijetae.com.

[9] S. Vasumathi Kannaki, "Secure data hiding using an integration of cryptography and cryptography", *Research Journal of Computer Systems Engineering,* vol. 4, June 2013. Available: http://technicaljournals.org//RJCSE.

[10] B. Schneier, Applied Cryptography, John Wiley and Sons, New York, 1994.

[11] B. Schneier, "Description of a new variable length key, 64 bit-block cipher(Blowfish)", in *Proc*. *Fast Software Encryption, Cambridge Security Workshop,* Springer-Verlag, pp. 191-204, Dec. 1993.

[12] Moulin P and Koetter R, "Data-hiding codes", Proceedings of the IEEE, 93 (12) (2005) pp. 2083-2126.

[13] Krenn. R., Steganography and Steganalysis , http://www. krenn.nl/ univ/cry/steg/article.pdf.

[14] Shannon C.E, Communication theory of secrecy systems, *Bell System Technical Journa*l, pp. 656-715, 1949.

[15] Burger W. and M. Burge, Digital Image Processing: An Algorithmic Introduction Using Java, Springer-Verlag, New York, 2008.