Image Encryption Using Block Cipher Based Serpent Algorithm

Dr. Yossra Hussain Ali
Computer Science Department, University of Technology/Baghdad.
Email: yossra_1@yahoo.com
Haider Aabdali Ressan
Email:haider_aleed@yahoo.com
Computer Science Department, University of Technology/Baghdad.

Received on:18/5/2015 & Accepted on:17/12/2015

ABSTRACT

In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. A proposal algorithm for images protection is depending on the block cipher serpent algorithm in feistel network structure, because numbers of round and linear transformation function and used block size of 512 bits rather than 128 bits has more complexity for attacker or unauthorized person to discover original images. In modified serpent, the correlation coefficient decreases to below the traditional serpent algorithm. When 64*64 pixel bitmap image is used the correlation coefficient for gray level between plain image and cipher image is (0.0023) in modified serpent and (0.0814) in traditional serpent.
Keywords: Encryption, Decryption, Serpent algorithm, type-3.

INTRODUCTION

Transforming and transmission of media substance sovereign unreliable systems has a few security Problem. Subsequently, sight and sound information security has turned into a genuine and significant issue in telemedicine, military, E-Commerce, budgetary exchange and cell telephone applications [1], [2]. To give security credits to sight and sound substance, one needs to ensure conveyed data (plaintext or pictures) from un approved clients. Sight and sound substance needs to be secured from diverse sort of assaults; for instance, intrusion, block attempt, alteration and manufacture [3], [4]. Cryptography is fundamentally scrambling of information for guaranteeing mystery and/or validness of data. Cryptology save media security from spy or basically the adversary while cryptanalysis manages the crushing such methods to recoup data or producing data that will be acknowledged as bona fide [4] . For secure transmission of media information, data ought to be hidden from foes or aggressors. Data is an advantage like different resources [1].The aim of this research is to design and implement an approach to protect the images by using a modification of the original structure in serpent block cipher algorithm to encrypt 512 bit blocks rather than 128 bit blocks. This approach depends on type-3 fiestel such as location permutation and secret key in block algorithm. This paper is introduced through : The introduction to security and theoretical background for cryptography including serpent algorithm ,discusses the new idea to image protection from unauthorized persons and attackers explains in some of flowcharts and algorithms the proposal structure depending on using the type-3 feistel structure and serpent block cipher algorithm as encryption function , presents the implementation of the structure including: interfaces of the program, results of tests to encryption and decryption images. Finally, there are some conclusions.

https://doi.org/10.30684/etj.34.2B.10
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Related Work

- **Ross Anderson et al., 1998 [5]**: proposed serpent block cipher as the AES candidate. It's highly conventional designed. It used S-boxes like to these of DES in other structure that concurrently allowed a extra quick avalanche, a more bit slice implemented, and simple analysis that enabled us to show the security against all recognized types of attack. used 128 bits a block size with a 256 bits key , it is fast like DES on the marketplace; yet believed it further protected than triple key DES.
- **Ashwaq T. Hashim, 2009 [6] :** had used The mystery key block cipher called 128-bits Blowfish which is a developmental change of 64-bits Blowfish intended to meet the prerequisites of the Advanced Encryption Standard (AES) to expand security and to enhance execution. This will be utilized a variable key size up to 192 bytes. It is a Type-3 Feistel system iterated basic capacity 16 times The proposed is performed on four 32-bit words.
- **Yossra H. Ali,2010 [7]:** had modified RC5. the highlight of 256 bits RC5 calculation is altered its plan to utilize four 64-bit enrolls instead of two 32-bit registers. This 256 bits RC5 calculation utilizing Type-3 Feistel system which is iterated basic capacity 20 times. This algorithm was impervious to coordinating and a lexicon assault which is expanded the security of the past RC5 algorithm by utilizing size of 256 bits rather than 64 bits.
- **S. G. Saravana Kumar, et al. , 2014 [8]:** The concept of Genetic Algorithm is introduced as a suggestion to modify fiestel network for the algorithm of Blowfish. This action has turned the encryption to be more complicated and not easily decrypted in the traditional way. The author has concluded that beyond the addition of new key and compensating the old XOR with novice one "#", the performance of Blowfish against any intrusion is improved and better results are gained.

Serpent Block Cipher Algorithm

The Serpent is a 128-bits block cipher and symmetric key size of 128, 192 or 256 bits, designed by Eli Biham , Lars Knudsen and Ross Anderson as a candidate for the Advanced Encryption Standard(AES). It was a finalist in the AES competition. Rijndael, the winner of AES, is faster (having fewer rounds) but Serpent is more secure. The Serpent is reiteration 32 once working on four words each one 32-bits thus make a128 bits block size. All values used in the cipher are represented as bit streams. This algorithm for cipher can explain as[7]:

- **First permutation** IP.
- **Redundancy**: Is 32, every comprising of a key blending operation, a go through S-boxes , and (in everything except the last round) a linear transformation. In the last round, this linear transformation is replaced by an additional key mixing operation,
- **Finishing permutation** FP.

The initial and final permutations do not have any import cryptography. They are used to simplify an optimized implementation of the cipher.

The Proposal Encryption

This work, proposes an approach for image encryption based on dividing the image to multi blocks of 512 bits, applying serpent block algorithm in type-3 feistel structure maps in order to meet the requirements of the secure image transfer. The proposed image encryption approach depends on modified serpent block algorithm by using type-3 feistel structure, and an external secret key. The initial conditions for both serpent and type-3 maps are derived using the external secret key by providing 33 different keys.

This approach divides n*n image into blocks each one is 512-bits then encryption by improved serpent. The 512 serpent approach makes use of data dependent on rotations. By using type-3 feistel network structure which is iterated simple function of 32 times.

The proposed encryption approach described in figure (1), where consist of four stages: The first stage is reading as RGB. bitmap image, the second stage is dividing into blocks each one is 512 bits, the third stage is ciphering each block alone which is used in proposal encryption approach and the last stage is writing collected blocks as image .

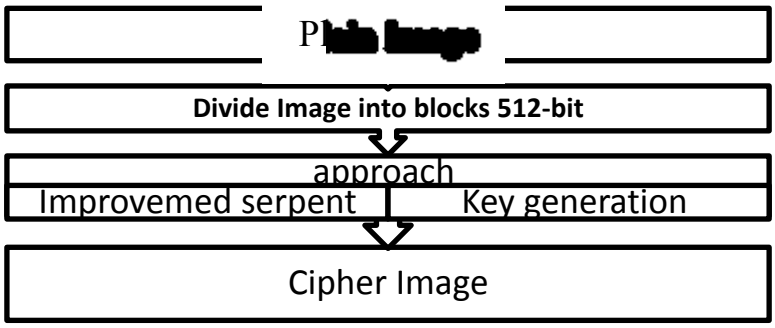

Figure (1): General Structure of Encryption

The modified Serpent use type-3 structure

After the divided ,each block 512-bits of permutation original image can process (encryption) by using the serpent of type-3 structure algorithm, by divide 512 bits into four 128 bits registers (A.B,C and D) then encrypt D with pervious serpent of one round encrypt D to get new register D' that encrypts with expand function to get R,M and L this is made exclusive or between (A with R), (B with M), (C with L), to get new registers B,C, D and A=D' respectively to iteration 32 round that is explained in figure (2) and algorithm (1) .

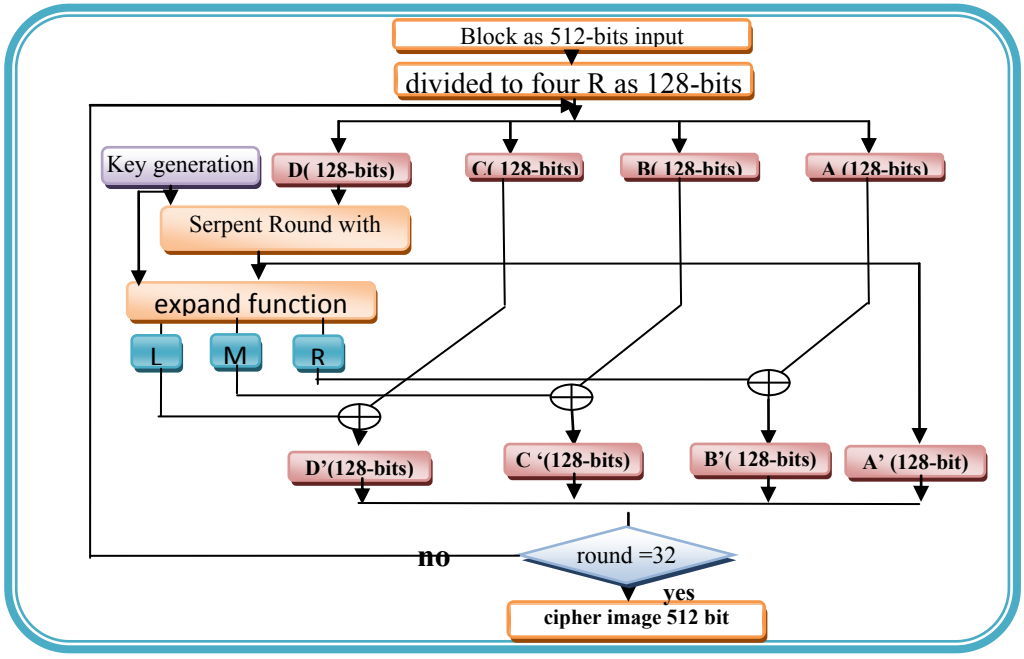

Figure (2) modified Serpent use type-3 structure.

Algorithm(1) modified Serpent use type-3 structure
Input: *Plain Register (A,B,C,D) as 128-bits:, key 256 bit*
Output: *Cipher Register (A', B', C', D') as 128-bits*
step 1: read Plain Register (A,B,C,D) as 128-bits *step2: read key 256 bit* *step3: for I=1 to 32 do* *3.1. Using key generator algorithm (2) with secret key to generate 33keys* *3.2. Using serpent algorithm with secret key to encryption D-128 bits register to find A' register 128-bits in one-round* *3.3. Using inverse modified serpent use type-3 structure algorithm (3) with secret key to expand encrypt A' register to find L,M and R* *3.4. D:=(C Xor L)* *3.5. C := (B Xor M)* *3.6. B :=(A Xor R)* *3.7. A := (A').* *Step4 D'=D , C'=C , B'=B , A'=A* *Step5 Return Cipher Register (A', B', C', D') as 128-bits*

The proposal Keys Generator

To generate 33 keys as 128 bit to use each one in different round by divide secret key 256 bit into two word as 128 bits and then generate 31 word by using the function : (*ki = (ki-2 XOR ki−1 XOR ϕ XOR i*) 31 times {when i is integer number 3< = i<=33 } .then split each one of this 33 key as four parts 32 bit to give132 parts process in S-box after that process it merge again each four parts as128 bit to get 33 new key .

Algorithm(2) Keys Generator
Input: Secret key 256-bits
Output: Array of secret keys (33 key) as 128-bits
step 1: Convert the key 256-bits to 2 k as 128-bits: *step2: For I = 0 to 255 Do step 128* *2.1. ki=mid (S,I, 128 bits)* *Step3: Generator 31 k as 128-bits form step4* *Step4: For I = 2 to 33 DO* *4.1. ki = (ki−2 XOR ki−1 XOR ϕ XOR i)* *4.2 Convert ki 128-bit to 4 32 word* *4.3.Convert 4 word (32-bits) to special values using S-Box, replace 4-bits from W with S-Box values ,where j permutation values* *4.4. New (Ka, Kb, Kc, Kd)= (S-Box) j (wa , wb , wc , wd)* *4.5. Ki (128-bits)= merge (Ka, Kb, Kc, Kd)128-bits*

The proposal E_function

The proposal Expand _function *(*E_function***)*** is using to more randomize in bits to expand encrypt of block , The E_ function use to product three registers L , M , and R (for left, middle and right) each one 128 pit from one register X 128 bit by split the key for the round into two

keys to use each key in some operation Initially, L will be set to hold the value of the source word rotated by 7 positions to the right, then XORed with key1,and R will be set to hold the L XORed with key2 then M will be set to hold the L XORed R and then rotated by 5 position to the right as in figure (3)

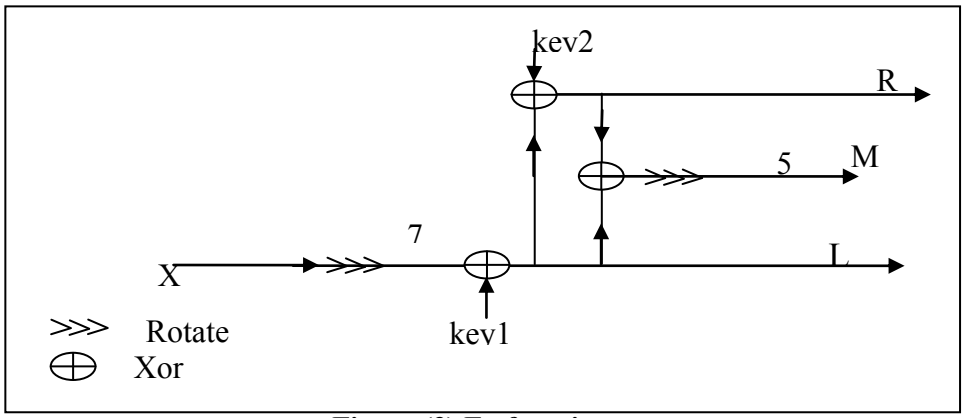

Figure (3) E_ function

The proposal Decryption

Decryption approaches the same structure of encryption with some inverse functions also explained in foure stages: The first stage is reading as RGB bitmap image, the second stage is dividing into blocks, everyone is of 512 bits, the third stage is deciphering each block using inverse proposed approach, the last stage writes collect blocks as image.

The Modified Inverse Serpent use Type-3 Structure

When the process in backward form to find the original block (plain block) must used the inverse process in the process must has the serpent algorithm and reverse order for type-3 structure to return the original register 512-bits,as show in figure (4) and algorithm (3).

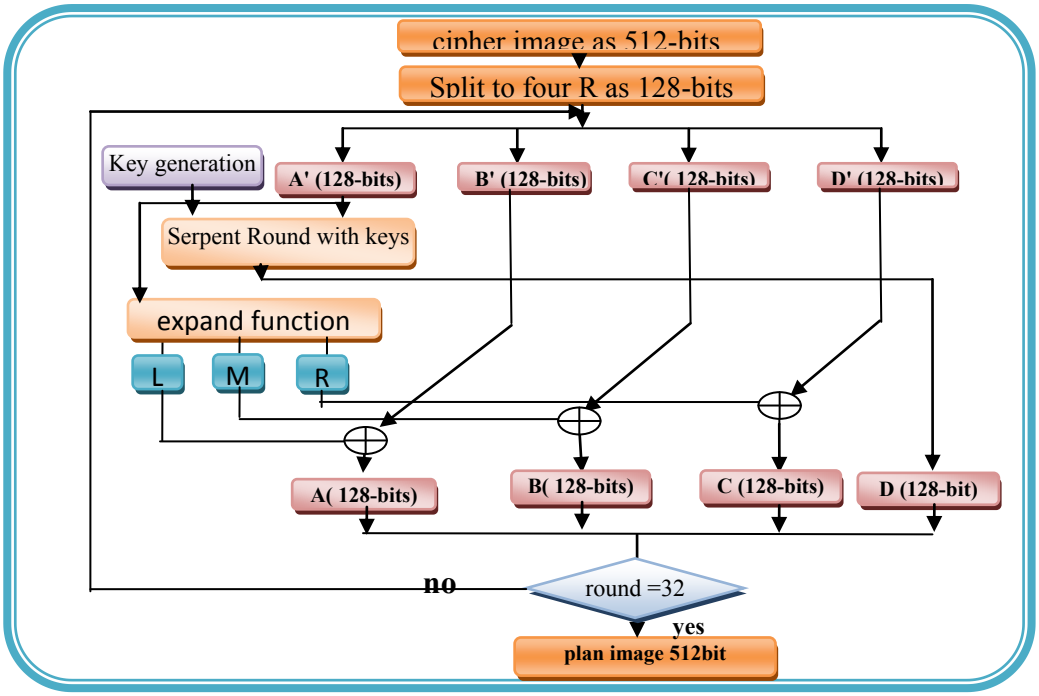

Figure (4): Inverse Modified Serpent Type-3 Structure Backwar

Algorithm (3) inverse modified Serpent use type-3 structure
Input: Cipher Register (A', B', C', D') as 128-bits, key 256 bit
Output: Plain Register (A,B,C,D) as 128-bits
step 1: read cipher Register(A', B', C', D') as 128-bits step2: read key 256 bit step3: for I=1 to 32 do 3.1. Using key generator algorithm (2) with secret key to generate key 3.2. Using inv serpent algorithm with secret key to encryption A'-128 bits register to find D register 128-bits in one-round 3.3. Using E_ function with secret key to encryption A'128 bits register to find L ,M ,and R registers each one 128-bits 3.4. A ' :=(B' Xor L) 3.5. B ':= (C' Xor M) 3.6. C':=(D' Xor R) 3.7. D':=D. Step4 A=A' , B=B' ,C=C' ,D=D' Step5 Return plain Register (A, B, C, D) as 128-bits

Serpent Algorithm Implementation for Encryption and Decryption Images

This algorithm present in detail in above need secret key 256-bit as 32 byte (hexadecimal)to generated 33 keys depend on keys generated algorithm for each round in improvement serpent algorithm to process each block from image . In the program interface can import of original image by file tools and save the encryption in storage disk, and enter the secret key in textbox as 32 hex to calculate the type of image, size of image, consume time to encryption process, entropy and correlation. and figure 5 take Lena bitmap image of (64*64) pixel as example to encryption approach : first show the plain image, second show cipher image use traditional serpent for encryption and last show cipher image use modified serpent for encryption.

Plain image	Cipher image in Serpent	Cipher image in Modified serpent
		

Figure (5): plain and encryption image

The Entropy of Proposed Structure

Entropy is measuring the insecurity relationship for random variables. A safe cryptic system should complete a condition on the information entropy that is the crypt image should not provide any information about the plain image and Table (1): explain the entropy for Lena and baboon bitmap images in old and new algorithm.

Table (1): The entropy bitmap images

Image	Image Size	Operation	Entropy for serpent	Entropy for modify serpent
Lena	64*64 pixel	Encryption Decryption	7.2341 7.4998	7.2341 7.5975
Baboon	64*64 pixel	Encryption Decryption	7.2216 7.5491	7.2216 7.6310

When calculate the entropy for Lena plain image is (7.2341) , the entropy for cipher image use traditional serpent (7.4998) and the entropy use modified serpent is (7.5975) .

The Correlation Coefficient Measuring Factor

To calculate the relationship between two variables use Correlation. If that variables are two image plain and its encryption, when the correlation equals to one if they are very dependent (identical). This case means the cipher image is the same as the plain image and this encryption method failed in hiding the details of the plain image. If the correlation coefficient equals zero, that mean plain image and its cipher are completely dissimilar, i.e., the cipher image has no features and highly independent on the original image. If correlation is equals -1, this means the negative cipher image is the plain image. So, success of the encryption process means smaller values of the correlation. The Table (2) and figure (6) explain the correlation for Lena and baboon bitmap images in old and proposed algorithm:

Table (2): correlation for bitmap images

Image	Image Size	Color	Correlation proposal	correlation
Lena	64*64 pixel	Red green blue	0.00734 0.00582 0.00546	0.01252 0.01594 0.01348
Baboon	64*64 pixel	red green blue	0.0023 0.009211 0.00993	0.01521 0.0110 0.0182

When calculate the Correlation between Lena plain and cipher image by use traditional serpent for red color level (0. 01252), green color level (0.01594) and blue color level (0.01348), and by use modified serpent for red color level (0.00734), green color level (0.00582) and blue color level (0.00546)

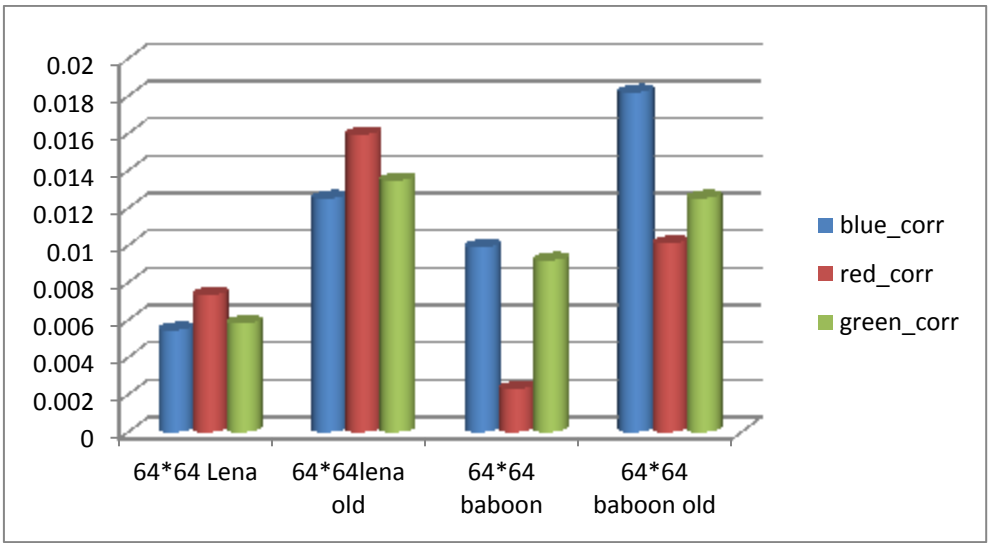

Figure (6): Correlation for bitmap image

Figure (6) explain the correlation deferent between old and modified serpent using lena and baboon image in red, green and blue color level .

The Image histograms Measuring Factor

Image histograms help in understanding the first order statistical behavior of the images. If there is no, or a negligible similarity, among the histograms of the original and cipher image, then the latter is considered secure from adversary attacks .

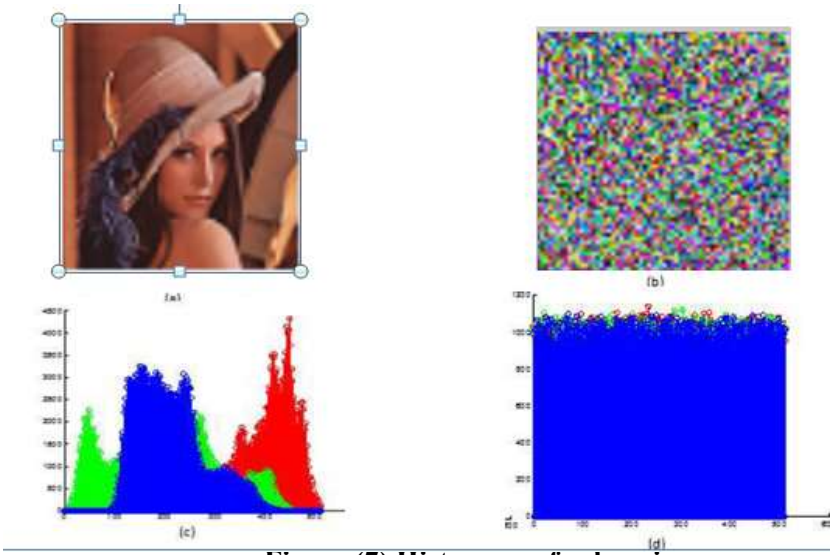

Figure (7) Histograms for lena image

.Figure (7) shows the histograms of Lena cipher images generated by proposed encryption algorithm and their corresponding plain images. It is clear that the histogram of the encrypted image is significantly different from the corresponding histograms of the original image. So, the encrypted image does not provide any hint to employ any statistical attack on the proposed encryption of an image procedure.

CONCLUSIONS

Several conclusions are reached through the system work steps. The following items represent the important conclusions which are drawn from the proposed system:

1. The 512 bit proposed algorithm increases the security and the complexity compared with traditional 128 bits Serpent algorithm.
2. The correlation coefficient in the 512bit proposed approach decreases compared with traditional 128 bits Serpent algorithm.
3. The proposed approach increases the degree of complexity against the attacker by consuming more time to achieve the analytical process which depends on number of keys used in Serpent function.
4. The degree of random images encoded depends on the type of the secret key. Generation of the random key leads to increased randomly encrypted image.
5. Type-3 feistel network as a proposed approach has a block length of 512 bits and word-size of 128 bits , it follows that each block consists of four words. Among the diverse network-structures which are capable of using four words in a block, it seems that a type-3 feistel network provides the best swap between speed, strength and correctness of analysis. A type-3 feistel network consists of many rounds, where in each round one data word (and a few key words) is used to modify all the other data words as compared with a type-1 feistel network

Recommendations

Based on the theoretical and practical stages of the proposed system, some techniques are proposed to be used as tools to enhance the system performance as shown below:

1. Embedding special information (in addition to the original information) in the secret image such as serial of credit card and biometric information to add new limitations against the attackers.

2. Using compression algorithm to give more speed where the proposed system is applied to other types of multimedia such as video and audio, to protect all component for secret multimedia channel.

REFERENCES

[1].B. Acharya, S. K. Patra, and G. Panda, "Image Encryption by Novel Cryptosystem Using Matrix Transformation," in Emerging Trends in Engineering and Technology, ICETET'08. First International Conference on, 2008, pp. 77-81 ,2008.

[2]. G. Jakimoski and K. Subbalakshmi, "Cryptanalysis of Some Multimedia Encryption Schemes," IEEE Transactions on, Multimedia, vol. 10, pp. 330-338, 2008.

[3].B. Schneier, “Applied Cryptography”. John Wiley & Sons, Inc., USA,1996.

[4].W. Stallings, "Cryptography and Network Security: Principles and Practice," Prentice Hall, 2011.

[5].R. Anderson, E. Biham, and L. Knudsen, "Serpent: A proposal for The Advanced Encryption Standard," NIST AES Proposal, vol. 174, 1998.

[6].A. T. Hashim, "Type-3 Feistel Network of The 128-bits Block Size Improved Blowfish Cryptographic Encryption," Eng& Tech, Journal, vol. 27, 2009.

[7].Y. H. Ali, "Proposed 256 Bits RC5 Encryption Algorithm Using Type-3 Feistel Network," Eng. and Tech. Journal, vol. 28, pp. 2337-2352, 2010.

[8].S. S. Kumar and A. Shanmugam, "Modified F–Function for Feistel Network in Blowfish Algorithm," International Journal of Engineering and Innovative Technology (IJEIT) Vol. 4, Issue 4, October 2014.