International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 4 Issue 8, August-2015

Cryptanalysis Resistant Image Security System

Lolla Chaitanya Sri Krishna[1], Anumula Deepthi Reddy[2], Vallapu Dinesh[3]

ABSTRACT

In the context of image security systems, literature reviews have shown that a combination of cryptography and steganography ensures greater security. However, the existing systems mainly deal with embedding secret data into an encrypted image with the drawback that recovery has to be done in the exactly reverse manner. Image information cannot be obtained until the embedded secret data is retrieved and revealed. In this paper, we have proposed two new schemes. In the first scheme, focus is on providing flexibility at recovery such that only the secret data can be retrieved by a certain group of people, image can be decrypted by another group and both by another group depending on which keys they are given access to. In the second scheme, focus is on providing higher security by first embedding the pre-encrypted secret message into a cover image and then encrypting the image. It gives a two layer security to the secret message and a sufficiently high security to the image. If confidential data is hidden in the image and then the image is encrypted, even if an intruder cracks the data-hiding key, he would extract an encrypted and meaningless message. In cases where the hidden data is confidential, encrypting the image misleads the intruder. He may try to retrieve the image but might not suspect the hidden message, adding more security to the message. Blowfish algorithm is used for implementing the image encryption part as it is highly resistant to cryptanalysis. Modified LSB substitution algorithm is implemented for embedding secret message into a image. The security strength of the proposed schemes has been checked by performing statistical analysis on the obtained results. The mean square error, PSNR, correlation and NPCR values proved that the performance of the designs is excellent. The subjected algorithms have resulted in a hundred percent decryption and produced good performance with lowest possible complexity in terms of data-hiding.

Keywords: PSNR, NPCR, LSB, Cryptanalysis, Statistical analysis, Blowfish, Data Hiding, Steganography, Cryptography.

I. INTRODUCTION

True to the word, the world has become a global village. Sharing information over the internet has become an inevitable part of daily life. However, sharing data over the internet has several "security concerns" turning the spot-light towards need for better "Data Security" strategies. Data Security means protection of data from unauthorized users or hackers while ensuring proper data at the destination. This area has gained lot of attention over the recent years due to massive increase in data transfer. In this paper, we are mostly concerned with Image Data Security Systems.

II. NEED FOR THE STUDY

Consider an example of military application where sensitive pictorial information is transmitted. In order to transmit this information, the images are converted into some non readable forms. Now this data is transferred across the network. But, with technology falling into the wrong hands, it is a child's play to hackers to understand the actual information. Due to this, various types of security attacks have come into picture. Even though the information reaches the receiver protected with some security system, the data might not be totally secure. There is a large possibility of the information being tapped or modified mid-way. Hence, there arises a need for high end security system.

III. OBJECTIVES OF STUDY

- To provide a high end security system which is resistant to security attacks.
- At the receiver end, there should be perfect retrieval without any errors.
- Provide flexibility to the receiver for data reception that is to support multi path communications.

IV. METHODOLOGY

A. EXISTING SYSTEMS

Literature review has shown that existing systems are as shown below [1].

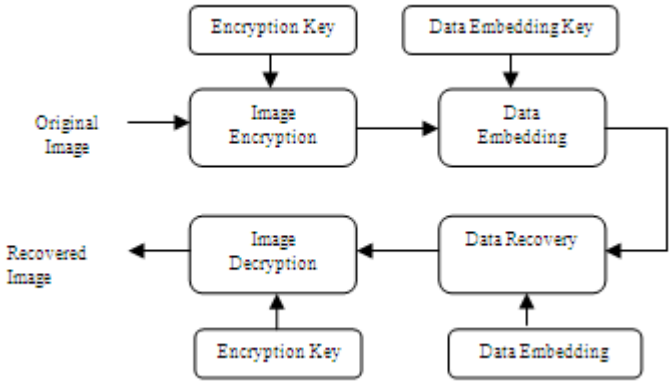


Fig. 1: Block Diagram of Existing Systems

In the existing systems, the image is initially encrypted using an encryption key. Later, the secret data is embedded into the image using the Data embedding Key. At the receiver side, the receiver needs to extract the secret data by using the secret key and then extract the sensitive image information. It is a serial process and not a separable process.

Hence, the major disadvantages include:

- Principle content of the image might be altered before decryption. (Lack of Protection).
- If someone has just Encryption key, he is unable to recover the pictorial information unless he performs recover. This has a lack of flexibility.
- Chance of loss of information at the receiver.

Hence in order to overcome those disadvantages, we proposed two new schemes: one deals with providing security as well as flexibility to the receiver. The other scheme deals with providing high end security system to overcome the disadvantages of the proposed scheme 1.

B. PROPOSED SCHEME 1:

In order to avoid the disadvantages in the existing systems, we provide a novel method which is more secure, has more flexibility and less chance of data loss of information at the receiver side. Suppose, the same encrypted image has to be transmitted all over the network, but a certain group of users are permitted to view the embedded data and possess the data embedding k, another group of users are permitted to view the encrypted image and hence possess the encryption key. Yet, another group has permission to view both the information and have access to both keys that is when this proposed scheme has an advantage over the existing schemes. To make it stronger than the previous systems, we used a strong algorithm called as blowfish algorithm. To provide flexibility at the receiver end, we introduced a new scheme of recovery. In this phase, if we have the data embedding key we can recover only the text. If we have the encryption key, the receiver can retrieve the image contents. If he has both the keys he can get both the information. Even if the information has undergone security attacks, it is difficult to retrieve the information as the encryption scheme used in this method requires around 2^{32} to 2^{448} guesses order to retrieve the information.

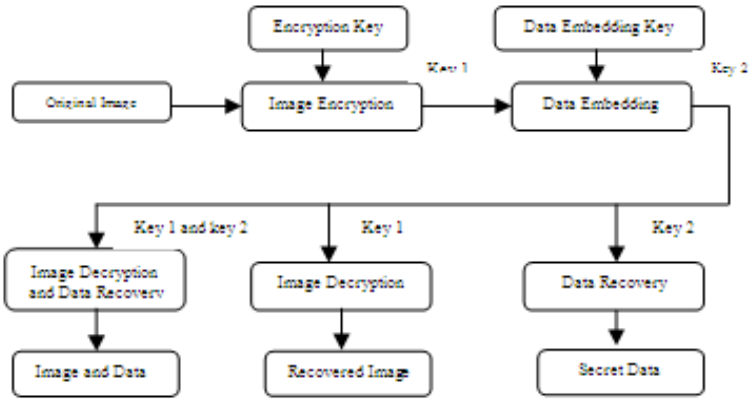


Fig. 2: Block diagram of Proposed Scheme 1

C. PROPOSED SCHEME 2:

In the existing systems, it is clear that we need to perform the procedural methods that is, Encryption and then followed by Data Hiding in order to make an image secure. Now there arises a case when both the pictorial and embedded information are highly confidential. Suppose, if a hacker tries to guess the data which is present in the encrypted image by collecting the least significant bit positions, then the secret information is lost. This may create huge damages. Hence in order to make the secret data secure, we can perform an additional encryption stage for the data using a strong encryption algorithm. But this is tedious. So we propose a novel scheme in which the data is embedded in the first stage in an image, and then the encryption stage using blowfish is followed. In this case, the data embedded in this image will undergo encryption stage which ignores the additional step as mentioned above. This provides an added security for both image as well as confidential data.

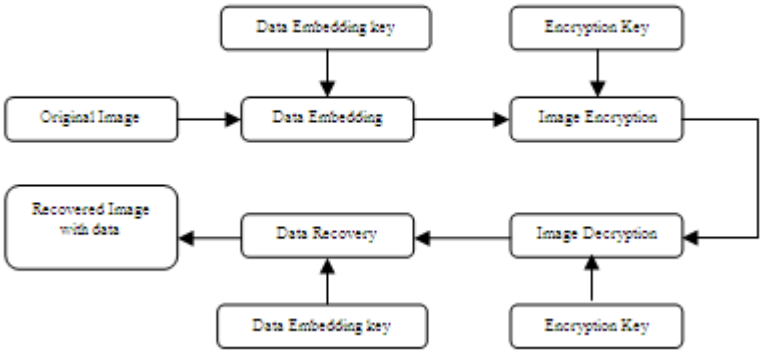


Fig. 3: Block Diagram of Proposed Scheme 2

V. IMAGE ENCRYPTION

The algorithm we have chosen to meet these requirements is "Blowfish Algorithm" which is proved to be more secure than DES, 3DES and RSA algorithms [2]. There has been no security breach to this algorithm till date making it one of the best encryption algorithms so far [3].

Blowfish Algorithm is a Feistel Network, designed by Bruce Schneier in 1993, iterating a simple encryption function 16 times. It is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data [4].

Blowfish Algorithm:
This algorithm is divided into two parts namely:

1. Key Expansion part
2. Data Encryption part.

A. Key expansion:

a) Key:

The strength of this algorithm is affected significantly by the strength of the key. Its length is variable making any attempt to guess the key size futile. Its length ranges from 32 to 448 bits. So, assuming the smallest key usage, the minimum number of guesses to be made will be 2^{32}.

b) Sub-keys:
The blowfish algorithm has two sets of sub-keys.

- The first set is the P-array (Permutation Box) consisting of eighteen 32-bit keys.
  P(1), P(2), P(3)……. P(18).
- The second is a set of four 32-bit S-boxes (Substitution Boxes) each having 256 entries.

S1(1), S1(2), S1(3),……S1(256).
S2(1), S2(2), S2(3)……S2(256).
S3(1), S3(2), S3(3)……S3(256).
S4(1), S4(2), S4(3)…….... S4(256).

c) Initialization and expansion:

The P-array and S-boxes are filled with a fixed string. Common practice is to use the decimal digits of PI in hexadecimal format as the fixed string. Form equivalent key by repeating the key till the required length is achieved. That is, if X is the key, XX, XXX, XXXX are called equivalent keys. The required length is nothing but the length required to XOR all the bits of P-array with consecutive bits of the equivalent key. XOR P-array with the equivalent key. Encrypt an all-zero string of 64 bits with the blowfish algorithm using the sub-keys available. Replace P (1) and P (2) with the result obtained. Now repeat step-II, that is, encrypt P(1) and P(2) using the updated P-array. Replace P (3) and P (4) with the result obtained. Repeat the process till all entries of P-array and S-box are updated. This completes the generation of sub-keys.

B. Data encryption

In this phase, data is handled in 64 and 32 bit blocks. Since blowfish is a 64 bit block cipher, the image data in blocks of 64 bits are sent as input to the encryption function and an encrypted block of 64 bits is given as output. The received blocks are re-arranged as an image, forming the encrypted image [5].

Algorithm:
This algorithm has 16 iterations for each block and it involves a round function denoted by F.

1. Input X(64-bit data block: original data)
2. Divide X into two 32-bit halves : XL and XR
3. For i=1 to 16:
   XL = XL XOR P (i)
   XR = F (XL) XOR XR
   Swap XL and XR
   End for
4. Swap XL and XR (Undo the last swap.)
5. XR = XR XOR P(17)
   XL = XL XOR P(18)
6. Recombine XL and XR
7. Output X (64-bit data block: cipher data).

Decryption is exactly reverse to the encryption process taking the arrays starting from P(18) to P(3), and finally the left block with P(1) and right block with P(2). This gives back the original image with 100% retrieval.

Round Function (F):
The F function is the kernel and distinguishing feature of Blowfish .The F Function, regarded as the primary source of algorithm security, combines two simple functions: addition modulo two (XOR) and addition modulo 232.

Algorithm:
1. Divide XL (32 Bits) into four 8-bit quarters: a, b, c, and d.
2. F(XL) = { { (S1[a] + S2[b]) S3[c] } ⊕ + S[d] },

Where + means addition modulo232, and ⊕ means XOR.

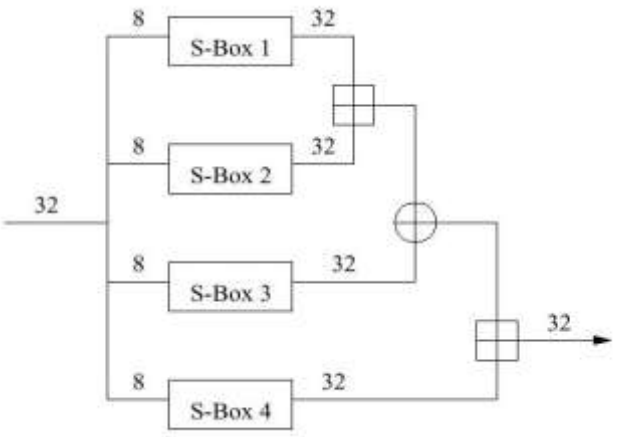


Fig. 4: Implementation of F function.

VI. DATA EMBEDDING:

In order to embed the data, we used LSB substitution algorithm [6]. As it doesn't provide good security to the data, we have modified the algorithm and provided security to the algorithm in our new algorithm (Modified LSB Substitution Algorithm).

Modified LSB Substitution:
We have divided the algorithm into two stages:

1) Encryption of Data with the key.
2) LSB Substitution into the image.

Encryption of Data with the key:

Step 1: Load the image.
Step 2: Read the text which is to be embedded into the cover image.
Step 3: Read the key that encrypts the text message.
Step 4: Repeat the key, that is, expand the key until it reaches the length of the text.
Step 5: Perform bit-wise XOR operation to encrypt the data with the text.
This stage encrypts the text that should be embedded into the image.
LSB Substitution into the Image:
Step 1: Convert the encrypted text into binary form.
Step 2: Replace the LSB of pixels in the image with the secret encrypted image.
Step 3: This forms the data embedded image.
Now it completes the Data Embedding Part.

VII. RECOVERY

The main of objective of recovery stage is to retrieve the information perfectly, without any errors and we achieved excellent results.

A. Recovery in Proposed Scheme 1:

- If the receiver has encrypted key, he can retrieve the image sensitive information.
- If the receiver has data embedding key, he can retrieve the data which is embedded.
- If the receiver has both the keys, he can retrieve both the information.
- If he doesn't have any key, he can't get the information as the algorithm we used is the most secure algorithm which is not broken till now.

B. Recovery in Proposed Scheme 2:

In the proposed scheme 1, we can also encrypt the text that is embedded into the image using blowfish algorithm. But this increases the complexity. Hence in order to decrease the complexity and provide additional security to the data (text, image or audio files) we move to proposed scheme 2.

Here, at the transmitted side we perform Data Embedding and then followed by Image encryption. Hence in the receiver side, the data should be retrieved in a sequential order : that is decrypt the image using encryption key and then extract the text using data embedding key. Though this lacks the objective of flexibility is gives added protection to data and image than the previous scheme.

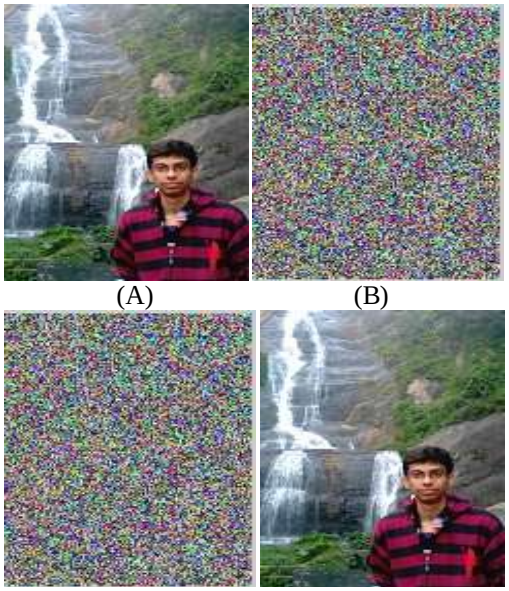
VIII. STATISTICAL ANALYSIS

In order to prove the resistivity of the image security system, we have performed some statistical analysis based on 3 factors:

a) PSNR: The peak signal to noise ration low values implies our system is efficient.
b) Correlation: Correlation low implies our system is efficient.
c) NPCR: Number of Pixel change rate which implies, the pixel changes that many times which is resistant to security attacks.

i. Statistics on RGB Images (Random Picture (160x120)) For Scheme 1

Encryption Key: project
Secret Text: students
Embedding Key: cvr



(A) (B)

(C) (D)

Fig 5: Results of the Random Picture.

A) **Original Image (160x120)**
B) **Encrypted Image before Data Embedding.**
C) **Encrypted Image after Data Embedding.**
D) **Decrypted Image.**

TABLE 1: PSNR CALCULATION

Images	**MSE**	**PSNR**
Original Image Vs Encrypted Image before Embedding	101.9093	28.0487 dB
Original Image Vs Encrypted Image After Embedding	101.9090	28.0487 dB
Original Image Vs Decrypted Image.	0.00000	Infinite
Original Image Vs Decrypted Image with Data Embedded	0.17900	55.6024 dB

TABLE 2: CORRELATION BETWEEN IMAGES

Images	**Correlation Value**
Original Image Vs Encrypted Image before Embedding	0.0049
Original Image Vs Encrypted Image After Embedding	0.0049
Original Image Vs Decrypted Image.	1.0000
Original Image Vs Decrypted Image with Data Embedded	0.9995

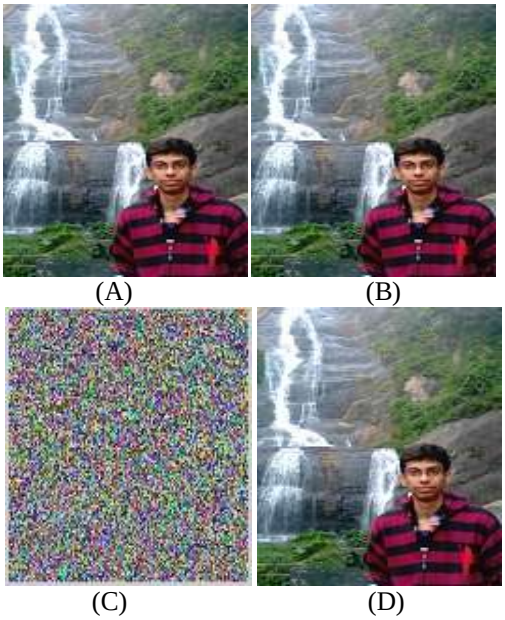
TABLE 3: NUMBER OF PIXEL CHANGE RATE (NPCR)

Images	**NPCR**
Original Image Vs Encrypted Image before Embedding	40.7917
Original Image Vs Encrypted Image After Embedding	40.7917
Original Image Vs Decrypted Image.	0.00000
Original Image Vs Decrypted Image with Data Embedded	0.22400

Thus, the obtained statistics prove that the proposed scheme-1 has met the security objectives.

ii. Statistics on RGB Images (Random Picture (160x120) For Scheme 2

Encryption Key: project
Secret Text: students
Embedding Key: cvr



(A) (B)

(C) (D)

Fig. 6: Results of the Random Picture.

A) **Original Image (128 x 128)**
B) **Image after Data Embedding.**
C) **Encrypted Image after Data Embedding.**
D) **Decrypted Image.**

TABLE 1: PSNR CALCULATION

Images	**MSE**	**PSNR**
Original Image Vs Data Embedded Image	2.2569e-04	84.5956dB
Original Image Vs Encrypted Image After Embedding	102.2002	28.0363dB
Original Image Vs Decrypted Image.	2.2569e-04	84.5956 dB

TABLE 2: CORRELATION BETWEEN IMAGES

Images	**Correlation Value**
Original Image Vs Data Embedded Image	1.0000
Original Image Vs Encrypted Image After Embedding	0.0103
Original Image Vs Decrypted Image.	1.0000

TABLE 3: NUMBER OF PIXEL CHANGE RATE (NPCR)

Images	NPCR
Original Image Vs Data Embedded Image	0.00000
Original Image Vs Encrypted Image After Embedding	41.1094
Original Image Vs Decrypted Image.	0.00000

The statistical analysis proves that proposed scheme-2 provides excellent security that can with stand security attacks.

CONCLUSION

In this paper, two designs for image securities using cryptography and steganography have been designed and implemented. Encryption has been implemented by using the blowfish algorithm that could not be cracked by security attacks till date. The modified LSB algorithm provided sufficiently good results even though it is of very low complexity. The results have been verified using statistical analysis of MSE, PSNR, correlation and NPCR values. The performance of the systems was found to be excellent and the statistical analysis proves that they are resistant to several cryptanalytic attacks.

REFERENCES

[1]. W. Puech, M. Chaumont and O. Strauss, "A reversible data hiding method for encrypted images," IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents, San Jose, CA : United States".
[2]. Milind Mathur and Ayush Kesarwan,"Comparison between DES , 3DES , RC2 , RC6 , Blowfish and AES," Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.
[3]. Pia Singh, "Image Encryption and Decryption Using Blowfish algorithm in Matlab," ISSN 2229-5518, IJSER Volume: 4, Issue 7, July-2013
[4]. Pratap Chnadra Mandal, "Superiority of blowfish algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.
[5]. Irfan.Landge, Burhanuddin Contractor, Aamna Patel and Rozina Choudhary, "Image encryption and decryption using blowfish algorithm, "World Journal of Science and Technology 2012.
[6]. Mrs. Kavitha, Kavita Kadam, Ashwini Koshti and Priya Dunghav ," Steganography Using Least Signicant Bit Algorithm," International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-June 2012.