Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on Image Encryption Technique based on Hyper Image Encryption Algorithm

Prachi Junwale[*] , R. Manasa Annapurna, G.Sobha
Asst. Prof, CSE ,MLRIT, Hyderabad
India

Abstract— Image applications have been increasing in recent years. The protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. In this paper, the original image divided into blocks, which were rearranged in to a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Hyper Image encryption techniques i.e. Blowfish algorithm. Finally we get a result as encrypted image that can be transferred over a network. This technique gives high security, flexibility, time efficiency and robustness.

Keywords— Computer network, Network security, Cryptography, Encryption, Decryption.

I. INTRODUCTION

Cryptography is well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence [1]. These techniques have many applications in computer science and other related fields. They are used to protect e-mail, messages, credit card information, corporate data, etc.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication [2]. Fig.1 shows steps for image encryption and decryption Image encryption has a wide range of applications in inter-net communication, multimedia systems, medical imaging, tele-medicine, and military communication. There already exist several image encryption methods like SCAN-based methods, chaos-based methods, tree structure-based methods, and other miscellaneous methods [6]. However, each of them has got their own strengths and weakness in terms of security level, speed, and stream size metrics. Hence, we now propose a new encryption method that would make an attempt to address the above mentioned problems [7].

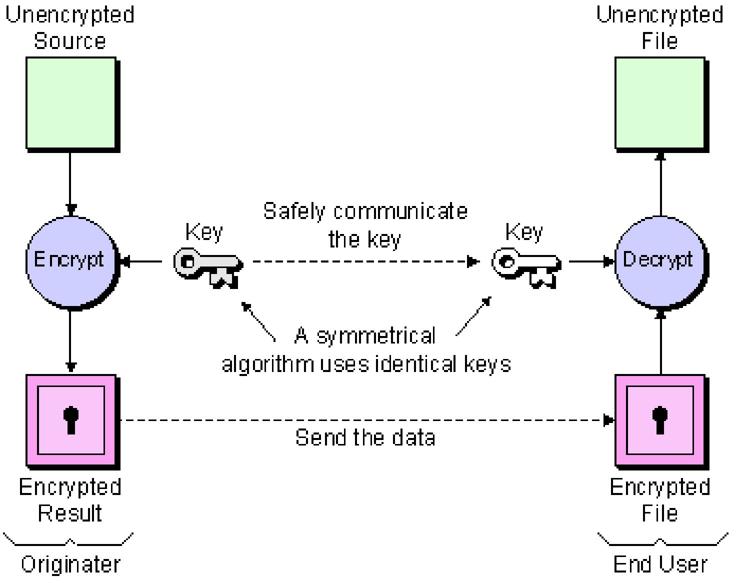

Fig. 1: Image encryption and decryption steps

II. BACKGROUND

Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Most of the algorithms specifically designed to encrypt digital images were proposed in the mid-1990s. There are two major groups of image encryption algorithms:

- Non-chaos selective methods
- Chaos-based selective or non-selective methods

However, most of these algorithms are designed for a specific image format, either compressed or uncompressed [1]. These are methods that offer light encryption (degradation), while offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption. The user is expected to choose a method based on its properties, which will be best for image security[4]. In modified AES based algorithm for image encryption 2007 author analyze the advance encryption standard and in their image encryption technique they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance. AES is very fast symmetric block algorithm especially by hardware implementation [5]. There are several image encryption methods like tree structure-based methods, SCAN-based methods, chaos-based methods, and other miscellaneous methods. However, each of them has got their own strengths and weakness in terms of security level, speed, and stream size metrics [2]. Hence, we propose a new encryption method that would make an attempt to address the above problems.

III. PROPOSED WORK

A. Proposed Technique

Initially in proposed image encryption system requires .bmp or jpeg type of image file that is to be hidden. It has two modules encrypt and decrypt shown in Fig. 2. Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simples programming. Here we used some .net tool in this software called “Image Crypto System (ICS)” that is written in VB.Net language and we can use this software to hide our visual information in .bmp or jpeg type of pictures.

Encryption is the the process of encoding messages (or information) in such a way that third parties cannot read it, but only authorized parties can. Encryption doesn't prevent hacking but it prevents the hacker from reading the data that is encrypted. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext (ibid.) [3]. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message [4]. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, that adversaries do not have access to it.

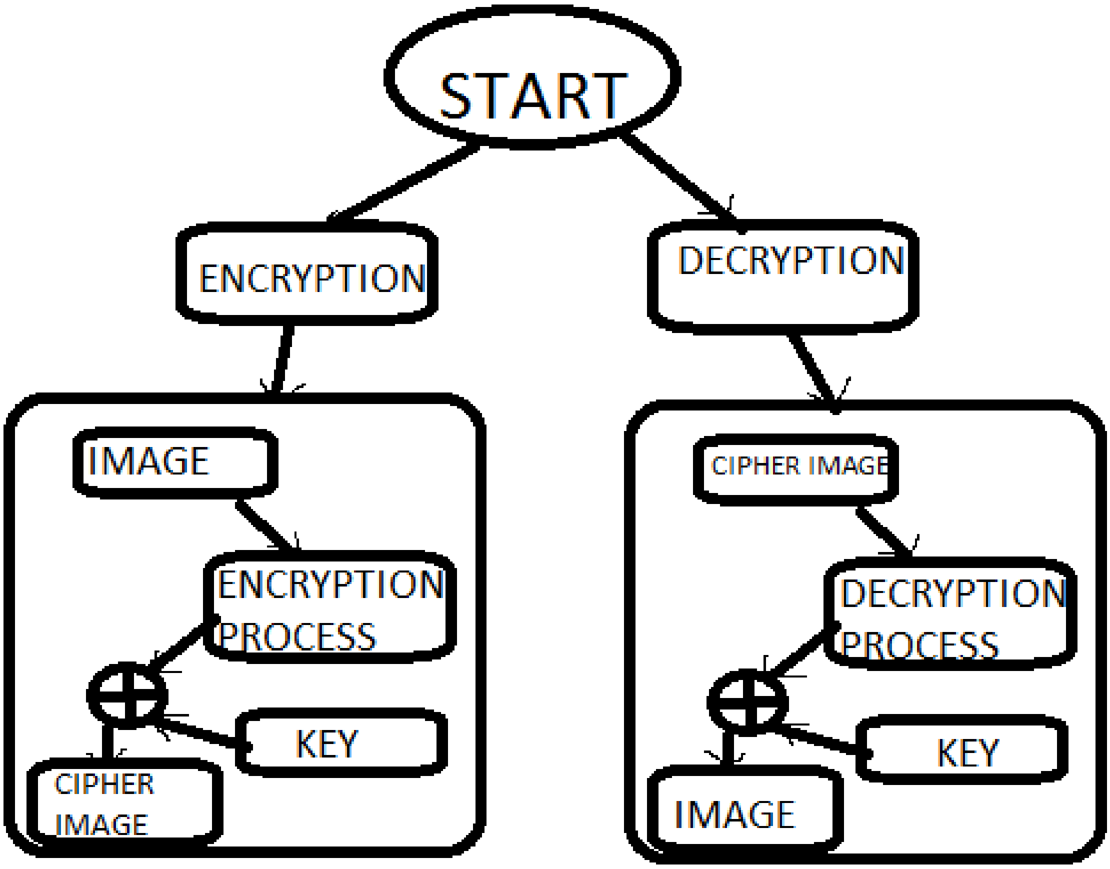

Fig 2: Graphical Representation of proposed system

B. Proposed Architecture

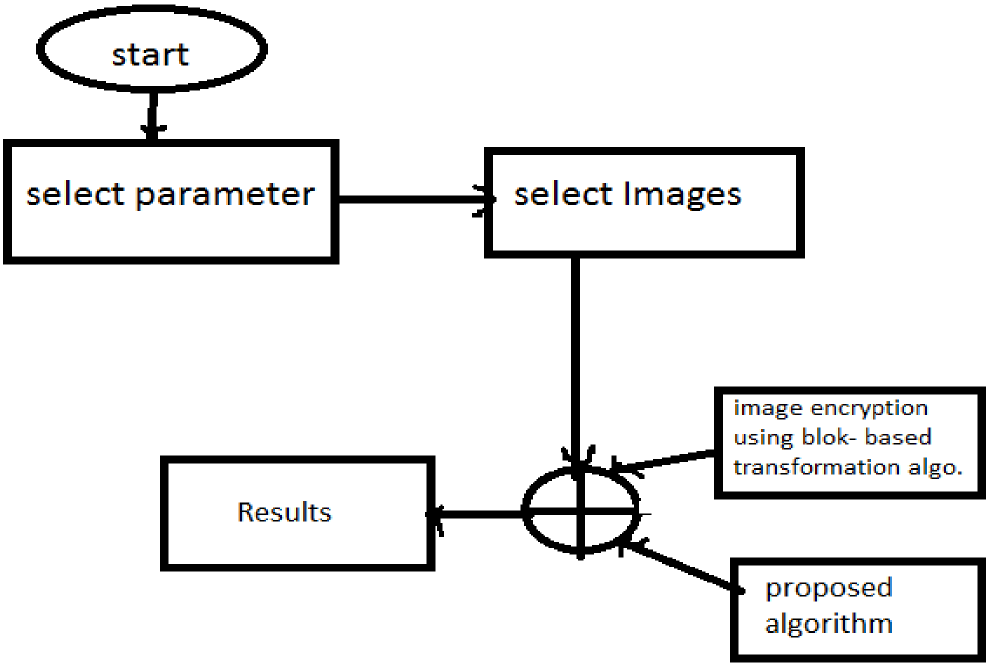

Fig 3: Proposed architecture

Proposed architecture is shown in Fig. 3. In this, we select parameters from huge database. Then, we can select image that is to be encrypt and to be send over communication network. Hyper Image Encryption Algorithm and block-based transformation algorithm are used to encrypt selected images.

Steps for creating Transformation Table:

1) Select an image
2) Divide image into pixel blocks
3) Calculate Horizontal Pixel Block = Image Width/10
4) Calculate Vertical Pixel Bloc = Image Height/10
5) Calculate Number of Pixel Blocks = Horizontal Pixel Block * Vertical Pixel Block
6) If Number of Pixel Blocks / 2 != 0
Then set Number of Pixel Block = Number of Pixel Blocks + Extra Pixel Block
7) Divide Number of Pixel Blocks into two equal Sub-Block (Sub-Block1 and Sub-Block2) respectively.
8) Select variable I =0 and R=0 (R ≠ Random Variable)
9) While I < Sub-Block1
R = Random Number between (0, Sub-Block1-1) Set new location of block R ≠ Pixel-Blocki (Selection of Pixel Block from Sub-Block1 Sequentially) I = I + 1 End While
10) Similarly for Sub-Block2. I =0 and R=0
While I < Sub-Block2 R = Random Number between (0, Sub-Block2-1) R ≠ Pixel-Blocki (Selection of Pixel Block from Sub-Block2 Sequentially) I = I + 1 End While
11) Finally we get the new location of pixels block in Sub-Block1 and Sub-Block2.
After creation of the transformation table we have applied proposed encryption algorithm.

Steps for Proposed Encryption Algorithm:

1) Select an Image which is having at least 256 bits in Size to be encryption.
2) Calculate Binary Value of Image.
3) Select First 256 bits form Binary Value and create 16 subblocks of 16 bits. This process will repeat till end of file.
4) Select Key Value of 256 bits. And create 16 sub blocks of 16 bits.
5) Select 64 bits from transformation table. And create 4 blocks of 16 bits.
6) Apply XOR Logical operation between first 8 block of selected image and second 8 block of selected key. Result will stored in image blocks.
7) Apply XOR Logical operation between last 4 blocks of selected images and 4 blocks of transformation table. Result will store in image blocks.
8) Apply Circular Shift Operation on last 4 block of selected key and second last 4 block of selected image.
9) Apply logical XOR operation between selected image and key which is output of step 8. Result will store in image block.
10) Apply Circular Shift Operation on 4 blocks of transformation table and second last 4 block of selected key.
11) Apply logical XOR operation between transformation table and selected key, which is output of step 10. Result will store in key block.

12) Combine output of step 6, 7, 9, and 11 in such that it should be produced 256 bits total. Output of this step will become input for next round.
13) Repeat step-1 to step-12, 10 times.
14) After 10th round, cipher text will produce of selected image.

Features of Proposed Algorithm:

- Proposed algorithm is very simple. Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.
- Due to the length of the key proposed technique is very much secured.
- Due to simplicity proposed technique is high efficient. To produce stronger ciphers our proposed symmetric key can be a good choice. Symmetric-key encryption is perceived to have an extensive history [8].
- With the advances in technology it is of vital importance that encryption system is robust enough to withstand the advances in technology. The more an encryption technique relies on mathematics, the less the robustness.
- Users expect encryption to be immediate, otherwise the process is cumbersome. The time efficiency of proposed encryption technique measures in second to encrypt and decrypt information and it's very good [8].
- The flexibility issues of proposed encryption technique are very high which is referring to the use of keys and whether the key lengths are set, or whether different key lengths can be used.

IV. Result

This method of encryption can be applied to any of the formats of images like jpg, tiff, ppm, pgm, png from the browser option. Fig. 4 shows the Original Image, Fig. 5 shows the Encrypted Image using transformation and Hyper Image (Blowfish) algorithm.

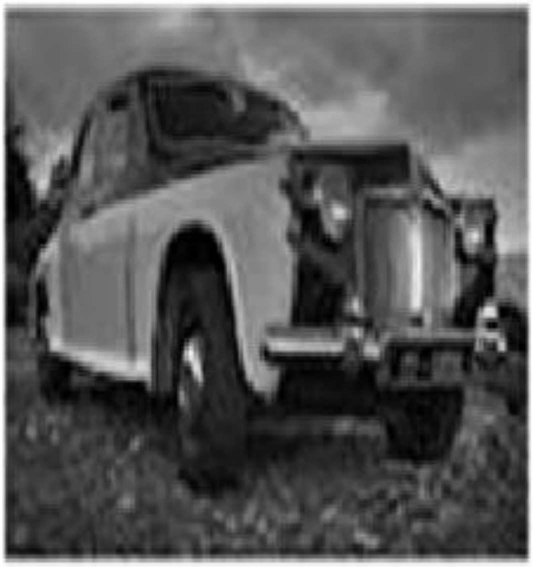

Fig. 4. Original Image

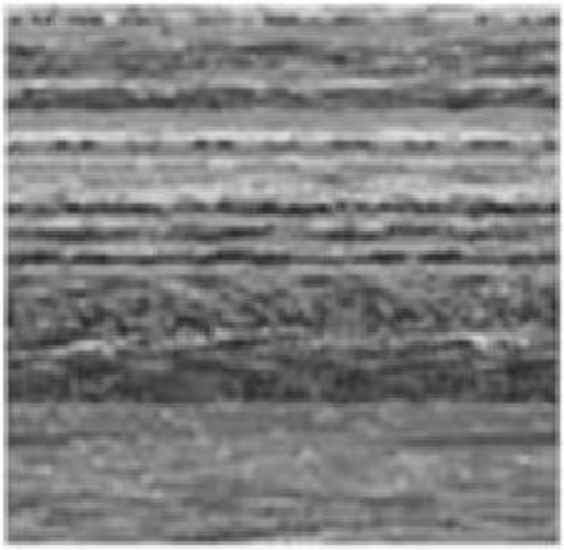

Fig. 5.Encrypted Image

V. Conclusions

In this paper, a better method has been proposed for image security using a block based image transformation and Hyper Image encryption techniques.The original image divided into blocks, which were rearranged in to a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm i.e. Hyper Image encryption techniques. And finely the result showed the correlation between image elements was significantly decreased .Their result also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation an higher entropy. In this algorithm there is no key generator .Here we use the Hyper Image encryption algorithm which divide image into number of blocks. Due to large data size and real time constrains, algorithm that are good for textual data may not be suitable for multimedia data. In this algorithm the correlation between image elements was significantly decreased.

Acknowledgment

The authors express their deep gratitude to the Principal and the Management members of MLRIT for their encouragement and extensive support in preparing and publishing of this paper.

References

[1] G. Zhi-Hong, H. Fangjun, and G.Wenjie , “Chaos - based image encryption algorithm," Department of Electrical and computer Engineering, *University of Waterloo*, ON N2L 3G1, Canada.

[2] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," *Journal of transactions on engineering, computing and technology* December, vol. 3, pp.38, 2004.

[3] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques,"*Journal of computer Science*, vol. 1(1), pp.127, 2006.

[4] Onwutalobi Anthony-Claret “Using Encryption Technique” Department of Computer Science, *University of Wollongong Australia,* Anthony.claret@ieee.org

[5] Prof. Mrinmoy Ghosh and Prof. Pranam Paul “An Application to ensure Security through Bit-level Encryption” *IJCSNS International Journal of Computer Science and Network Security*, VOL.9 No.11, November 2009.

[6] Mohammad Ali Bani Younes and Aman Jantan “Image Encryption Using Block-Based Transformation Algorithm” *IAENG International Journal of Computer Science*, 35:1, IJCS_35_1_03 Advance online publication: 19 February 2008.

[7] Mohammad Ali Bani Younes and Aman Jantan “An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption” *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.4, April 2008.

[8] Ratinder Kaur, V. K. Banga “Image Security using Encryption based Algorithm”, *International Conference on Trends in Electrical, Electronics and Power Engineering* (ICTEEP'2012) July 15-16, 2012 Singapore.