A Review of Image based Cryptography

Purvee Raghuwanshi M. Tech Scholar, Jijo. S. Nair, Assistant Professor
purvee.oct@gmail.com, jijosnair@gmail.com
Department of Computer Science & Engineering
Oriental Institute of Science & Technology, Bhopal

***Abstract*— Now a day we are dependent on websites or internet for sharing data from one user to another, from one place to another. It is very effective and easy for transferring information but it is very complex in terms of providing security. There are many algorithms which are being used to provide security in text and images. In this paper we study many cryptographic algorithms which are based on different parameters, like public key, private key cryptography and different images like Gray Scale Image, Colour Image, 2D Image, 3D Image, and Biometric Image. But all existing algorithms have some advantage and disadvantage. On the basis of existing methods we will develop a strong cryptography technique that will be very effective in terms of time and security.**

Index Terms— **Cryptography, 2D Image, Symmetric Key, Network level security, Encryption, decryption, 3D Image, private key.**

I. INTRODUCTION

The growth of internet, multimedia information is transmitted over the internet easily, Internet brings us much handiness, but it also gives an opportunity to attacker or intruder to hack our personal information, password, cookies etc. Generally two approaches are used for securing information. One is information hiding techniques like anonymity, watermarking, steganography etc. Another is cryptography.

"Cryptography is the process of protecting data by converting it into an unreadable format, called cipher text. This process of changing data into different form is known as encryption. The cipher text can be converted back to the original data with the help of secret key, this process is known as decryption". [7, 9].

A. The Need for Cryptography

Security often requires that data should be kept protected from unlawful access. And the best line of protection is physical security. But we always cannot use physical security as the only protecting medium. Instead, most computers are organized with each other explicitly, thereby displaying them and the communication channels used by them require-

- **Confidentiality:** It assures that private data remains private.
- **Authentication**: It assures that the characteristics of all parties attempting access.
- **Authorization:** It assures that a certain party attempting to carry out the process is allowed to do so.
- **Data Integrity:** It assures that an object is not distorted illegitimately.
- **Non-Repudiation:** It assures against a party denying a information or interaction that they initiated.

B. Key Based Cryptography

Nowadays, key based cryptography is mostly used in which string of bits is used to encode the original data into Secret message and back again to original data when required. There are two types of key based cryptography which depends upon the availability of the key publicly.

C. Private key Cryptography

In this both the sender and the receiver use the same key to encrypt or decrypt the data by keeping the key private. Passing key to the other side is an difficult task and a bit complicated to perform accurately. Examples of private key cryptography are Data Encryption Standard (DES), triple DES, RC2, RC4 IDEA and Skipjack. Other name of this cryptography is symmetric key cryptography [8].

D. Public Key Cryptography

In this both the sender and the receiver has two sets of keys; one is public key open to all and another is secret key which is known to the owner only. One who wants to communicate with other side, his data will be securely encrypted with the receiver's public key. And on the other side only those who have the matching private key can decrypt the original data. Example of Public key algorithms: Diffie-Hellman, RSA and Merkle-Hellman.

II. RELATED WORK AND BACKGROUND

Mr Niraj kumar et.al [2014] [1] has developed a new cryptographic algorithm to represent the multimedia content security in network channel. This algorithm represents the scheme for color image encryption in the framework that utilizes the 3D matrix. This algorithm is based on a new technology for key generation of images. Here a new key generation process is developed for encryption and decryption which is unique.

Two different public key is the use of cryptography process. [1, 7] Key generation function coding is different from encryption and decryption program due to hide values from the user and hacker. The performances of the encrypted and the decrypted images have been tested and the result has been analyzed through MATLAB simulator.

The proposed algorithm reduces the losses of image pixel during encryption and decryption. A lossless digital encryption model based on a new technology for key generation for images is proposed here [1]. The proposed algorithm is simple and difficult for the intruders to avail the key, but it need more computation time and power.

Quist-Aphesti Kester et.al [2014] [2] has proposed an encryption technique of securing the biometric image data collected from devices using AES and visual cryptography

method. Here author presented an approach of encryption of images using AES and visual cryptography [2, 10].

The key was extracted from the image features and the AES-256 algorithm was used to generate the key used for the image encryption based on the extracted key. The pixel values of the images to be encrypted were encrypted using n-share visual cryptographic technique. This encryption process experiences no loss of pixel values during the process.

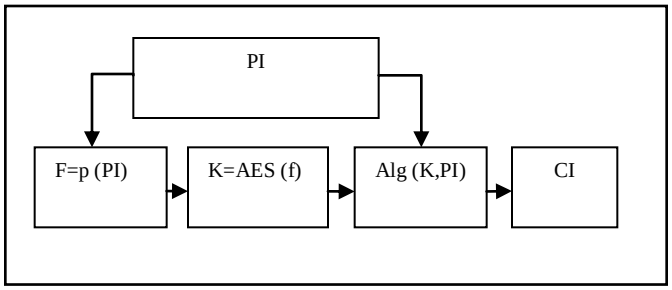

Figure 1: Process Diagram

This figure shows the whole process of the proposed method.

PI = plain image
F = extracted feature
K = key obtained from the extracted feature using AES
Alg = visual encryption algorithm employed
CI = ciphered image

Firstly the feature extraction process is carried then "The Rijndael - Advanced Encryption Standard Algorithm "is applied on the extracted feature. And finally the visual cryptographic encryption process is carried out.

The basic design and strength of encryption algorithm depends on diffusion and confusion. This engaged the use of Advanced Encryption algorithm and visual cryptography in securing forensic biometric images which resulted in linear and differential cryptanalysis.

Priyanka.M, Lalitha Kumari.R [2013][3]has concentrated on the structure of key generation procedure to be simpler to understand and also complicated to crack the key. Session based images are considered for key generation. Instead of storing and remembering the secret key, here images are stored in the database. This reliable and efficient security mechanism is to protect the information from the intruder. The figure 2.2 shows all the steps of encryption and decryption.

Our algorithm aims to transfer confidential information over a shared network .It includes the following steps:

A. Image Database:

In this phase, twenty four images are used on hourly basis. The images should be a color image. Once the sender and the receiver are ready for communication they will be given access to the image data base. Only authorized sender and receiver can access the image database.

B. Key Generation:

Key generation is based on the image stored in the database. Consider the pixel value of an image and extract one channel (RGB) at a time. It can be either a red channel or green channel or blue channel. The values of the components should be stored in an array. The array size should be p*q where p and q are the resolution of an image.

The key is generated based on the following steps. In the algorithm all the channels are considered for key generation.

1. Red channel: Consider only the diagonal values of the array whose indexes (N) are N%8=0.

i. The diagonal pixels thus considered are again stored in an array.

ii. RMS (Root Mean Square) value for those diagonal values are calculated

iii. RMS=$\sqrt{}$ ($a_{12}+a_{22}+a_{32}+...+a_{n2}$)/n, Where a=diagonal pixels stored in the array.

iv. The generated RMS value is considered as a part of the key and it is stored in a variable.

2 .Green channel:

i. Extract the green channel values and store it in an array.

ii. Sum up the all the pixel values in a zigzag manner starting from 0x0 to (n-1) x (n-1), n=size of the image and store the summed up value in a variable.

3. Blue channel: Repeat the steps of the red channel. Now, the value got using the red channel is appended with the value got using the green channel and the blue channel value is also appended to generate the key.

C. Encryption:

The sender encrypts the confidential message using the RC5 algorithm is showed in Fig 2. The key thus generated using image is given as input for the encryption. As the images are considered on hourly

Basis, if the encryption is done on nth hour then nth image in the image database is considered. Once the encryption is done it is sent to the receiver along with the session log. The session log contains the time in which the encryption is done.

D. Decryption:

In reference to the session log the receiver will consider the image in the image database to generate key for decryption. The generated key along with the encrypted message is sent for decryption (RC5 Algorithm) and the original message is extracted.

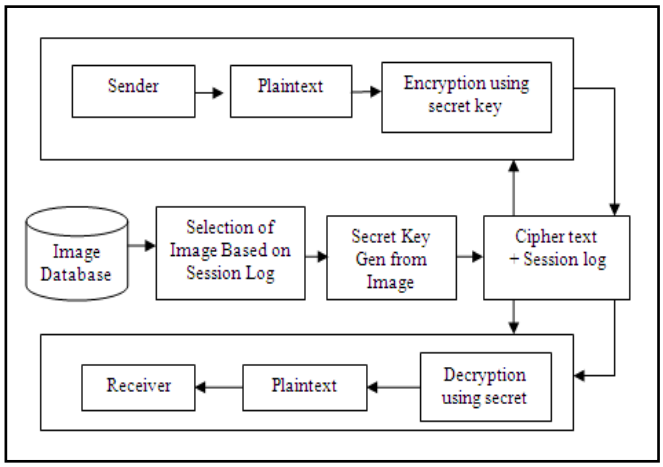

Figure 2.2: Architecture for the Session based key Generation

M. Y. R. Gadelha et. Al [2012] [4] has proposed the method in which the message is encrypted and decrypted using image and for performing the encryption firstly the ASCII value of each alphabet of the message is found in the key image and the similar ASCII value is searched and that location is being marked.[3, 8] After finding the location its location value is inserted in the corresponding cipher text of that message.

Similarly for performing the decryption the coordinate value is taken from the cipher text and reached to that location. The main reason behind the slower encryption time of the proposed algorithm is that, when the algorithm must encrypt an ASCII value with no corresponding pixel intensity in the key-image, it has to search for a pixel with the nearest intensity value. [7, 8] All the algorithms used in this method were implemented using MATLAB program.

The proposed method took an advantage of the random nature of pixel intensity values of an image. This method has a disadvantage of additional computational overhead to accomplish the data compression and it also has slower encryption time.

Gopi krishnan S et. Al [2011] [5] has proposed a new cryptographic scheme based on visual cryptography for securing color image [4, 5]. The proposed scheme is based on YCbCr color model. The encryption and decryption works with the help of half-tone and inverse half-tone respectively and based on visual cryptographic scheme.

A key binary image is generated by randomly distributed 4x4 matrices with equal number of O's and 1's randomly. To encrypt a color image, the image is decomposed as three monochrome images in tones of luminance, chrominance (blue), and chrominance (red). The half-toning technique, which is a reprography technique to convert a high color image into low color images is, applied on these monochrome images to reprography them into binary images.

This proposed method used Jarvis half toning method to half tone the images. Finally XOR operation is done between the Binary images obtained in half tone and shrae-1/key images. The proposed encryption algorithm uses only (M*N)/2 iterations. It generates random dotted matrix and perform XOR operation with secret binary half-tone images. Here author has presented an image cryptographic scheme based on visual cryptography for natural images.

This new scheme provides efficient computation to generate key and cipher. The space taken to store the binary key image and cipher image is lesser than the original secret image. The height and width of image retained constant throughout the process. Due to its robustness against few cryptographic attacks, it can be extended to work with identity based cryptography.

Jenifer Karunya et. Al [2011] [6] has explored an overview of visual cryptography used in secure transfer of images which are used by Google earth and Google maps collected by the satellite which are stored in image library. Related work is based on using binary logo and recovering secret image.

In this scheme, with the help of gray scale secret image a halftone image HI is created by using an error diffusion technique [4, 5]. A halftone logo HL is created of the HI by an interpolation technique. To ascertain the reliability of the reconstructed gray scale secret image 01 and the judgment of the set of collected shadows the HL created is used.[8, 9] the complete work is explained in 3 phases. The first is the shares construction phase, which creates two halftone shadows from a gray scale secret image GI. The second is the displaying phase, where the HL and gray scale secret image GI is generated. The third one is verifying phase, during which HI and HL is compared and if any cheating is there it will be discovered using human vision or the MSE value at last.

III. COMPARATIVE METHODOLOGY

Following table 3.1 shows the comparative study of existing methods with their parameters of research.

Table 3.1: Comparison of various existing techniques

S No.	Year	Name of Researcher	Method
1	2014	Niraj Kumar and Prof Sanjay Agrawal	Image Cryptography
2	2014	Quist Aphesti, Laurent Nana	Securing biometric image data using AES and visual cryptography method
3	2013	Priyanka.M and Lalitha Kumari.R	Image cryptography
4	2012	M.Y.R Gadhella, C.F.Costa Filho and M.G.F Costa	Data encryption using images that explore random spatial distribution method.
5	2011	Gopi Krishnan and Loganathan.	Visual cryptographic scheme
6	2011	John Blesswin and Rema	Visual cryptography techniques

IV. CONCLUSION

This work concluded the overall view about the existing cryptographic image based algorithms; all existing methods have some advantages and disadvantages on basis of time and security problems. Many researchers have developed various algorithms but none of them are efficient like 3D image cryptography. There are chances to improve the result of 3D image cryptography in near future. So we can develop an algorithm that is more secure and less time consuming as compared to existing algorithms.

REFERENCES

[1]. Niraj Kumar and Prof Sanjay Agrawal "An Efficient and Effective Lossless Symmetric Key Cryptography Algorithm for an Image" IEEE, Conference Publications, Pages1-5, DOI 10.1109/ ICAETR.2014.7012788.

[2]. Quist-Aphetsi Kester, Laurent Nana "Feature Based Encryption Technique For Securing Forensic Biometric Image Data Using AES and Visual Cryptography" 2014 Second International Conference on Artificial Intelligence, Modelling and Simulation, Pages 3-14, DOI 10.1109/AIMS.2014.65.

[3]. Priyanka. M, Lalitha Kumari. R, Lizyflorance. C and John Singh."A New Randomized Cryptographic Key

Generation Using Image" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013.

[4]. M. Y. R. Gadelha, C. F. F. Costa Filho "Proposal of a Cryptography Method Using Gray Scale Digital Images" The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012), Pages 7-8,IEEE.

[5]. Gopi Krishnan S and Loganathan D "Color Image Cryptography Scheme Based on Visual Cryptography" Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011) Pages 8-11, IEEE.

[6]. John Blesswin, Rema "Recovering Secret Image in Visual Cryptography" Pages 7-11,IEEE Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An imageEncryption approach based on chaotic maps"Department of Computer Science and Engineering, Chongqing University, Chongqing, China, 2005,759- 765 www.elsevier.com/locate/chaos].

[7]. S. Changxiang, Z. Huangguo, F. Dengguo, C. Zhenfu & H. Jiwu, "Survey of Information Security", Science In China Press 2007. H. Cheng, X. Li, "Partial Encryption of Compressed Images and Videos", IEEE Transactions on Signal Processing, Vol. 48 No. 8, August 2000.

[8]. R. Rudraraju, B. A, "Digital Data Security Using Encryption", Master's Paper, University of Texas at San Antonio, 2010."Emerging Cryptographic Challenges In Image And Video Processing Mitsubishi Electric Research Laboratories", TR2012-067 September 2012.

[9]. N. K. Pareek, Vinod Patidar, K. K. Sud, "Cryptography victimization multiple one-dimensional chaotic maps", Communications in nonlinear Science and Numerical Simulation 10 (2005) 715-723].

[10]. Philip P. Dang and Paul M. Chau "Image Encryption For Secure Internet Multimedia Applications" IEEE 2000;Department of Electrical and Computer Engineering, University of California, San Diego La Jolla, CA,@2000,92093 0098 3063/2000].

[11]. Secret Key Cryptography http://www.ggu.ac.in/ download /ClassNote14/public%20key 13.02. 14.pdf.

