A Survey Paper on Image Encryption Techniques

Monika Gunjal[1] Jasmine Jha[2]
[1] M. E. Student [2]Assistant Professor
[1]Department of Computer Engineering
[2]Department of Information Technology
[1, 2]L. J. Engg College, Ahmedabad, Gujarat, India

Abstract—Security is an important issue in digital data transmission and storage. The security can be provided by image encryption. Encryption is one of the ways to provide high security when images are transmitted over the network. Image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image which is hard to understand. There are so many different image encryption techniques available to protect confidential image data from unauthorized access. Image encryption techniques which provide transmission of digital images in more secure way. Encryptions algorithms that are good for textual data may not be suitable for multimedia data because images contain large data. This paper present survey of various encryption methods with its advantages and disadvantages.

Key words: Image, Encryption, Decryption, cryptography, Public key, Private key, facial-blurring, pixel, shuffling, visual cryptography, medical images, AES, Shifted Image, Entropy, correlation, Blowfish, DES, RGB,, Rearrangement,, sorting, pixel intensity, swapping, Digital Signature, RSA, SRNN.

I. INTRODUCTION

Information is transmitted over the internet in which it is very easy to disclose important information from theft so encryption techniques were used. Encryption techniques are very useful to protect secret information from unauthorized access. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code [10] .Mostly images are vastly used in today's world to represent information in various domains varying from corporate world, health care, document organization, military operations etc [1].Image encryption techniques convert original image into another image that is hard to detect called cipher image. Decryption is the reverse process of encryption in which cipher image is converted into original image by providing the key which is used in encryption.

Cryptography[11]*:* The many schemes used for enciphering constitute the area of study known as cryptography.

Types of Cryptography [11]*:*

There are two main types of cryptography:

1) Secret key cryptography
2) Public key cryptography

Secret key cryptography is also known as *symmetric key* cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Public key cryptography, also called *asymmetric key cryptography*, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. Cryptography technique is used when secret message are transferred from one party to another over a communication line. Cryptography technique needs some algorithm for encryption of data.

II. TECHNIQUES FOR ENCRYPTION AND DECRYPTION

A. Practical Approach on Image Encryption and Decryption Technique Using Matrix Transformation

This paper presented an Image Encryption and Decryption Technique Using Matrix Transformation. The proposed scheme is useful for encryption of large amounts of data, such as digital images. First, we use discrete cosine transformation to get a blocked image. Second, a pair of keys is given by using matrix transformation. Third, the image is encrypted using private key in its transformation domain. At the receiver side, the receiver uses the public key for decrypting the encrypted messages. This technique satisfies the characters of convenient realization, less computation complexity and good security. The salient features of the proposed asymmetric image encryption scheme can be summarized as: (a) Lossless encryption of image. (b) Less computational complexity. (c) Convenient realization.(d) Choosing a suitable size of matrix according to the size of image.(e) Encryption/decryption scheme uses integer arithmetic and logic operations. It requires minimized computational resources [5] .

B. A cryptographic image encryption technique for facial-blurring of images

This paper proposes an image encryption technique that will make it possible for selected facial area to be encrypted based on RGB pixel shuffling of an m*n size image. This will make it difficult for off-the-shelf software to restore the encrypted image and also make it easy for the law enforcement agencies to reconstruct the face back in case the picture or video is related to an abuse case. The implementation of the encryption method will be done using MATLAB. At the end, there will be no change in the total size of the image during encryption and decryption process. In this method, the facial selected portion of the image used will have their RGB colors extracted from then and then encrypted to have a ciphered image portion. The ciphering of the image for this paper will be done by using the RBG pixel values of the selected portion of the images. There are no changes of the bit values and there is no pixel expansion at the end of the encryption process. With the proposed method in this paper, the shuffling of the image will be ultimately done by solely displacing the RGB pixels and also interchanging the RGB pixel values[3] .

C. A Visual Cryptographic Encryption Technique for Securing Medical Images

This paper presented a visual cryptographic technique for encrypting of medical images before transmission or storage of them. This technique will provide protection of images from unauthorized access and also ensures confidentiality. This encryption technique based on pixel shuffling and a secret key generated from the image. In encryption process, an input image which was a plain image was operated on by a function to generate a secret key from it. The key was then used to encrypt the image by shuffling the pixels of the plain image based on an algorithm. After the encryption process, the ciphered image was obtained. The ciphered image can either be stored or transmitted over a communication network. To decrypt the image, the received image was then operated on again by a function to obtain the key. For the encryption and the decryption process, the proposed method combines visual cryptography with shared secret key. There were no changes of the bit values of the images used and there was no pixel expansion at the end of the encryption and the decryption process. Therefore there was no change in the total size of the image during encryption and decryption process. The characteristic sizes of image remained unchanged during the encryption process[4] .

D. Image encryption and decryption using blowfish algorithm in MATLAB

This paper implementing blowfish algorithm which is strongest and fastest in data processing and storing compare to other algorithms. Blowfish algorithm has longer key length so it provides high security. The main aim behind the design of this proposal is to get the best security/performance tradeoff over existing Web Images. As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. In Blowfish algorithm, the left and right 32-bits of data are modified at each round while in DES The right 32-bits of data are modified only to become the next round's left 32-bits.But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits[6] .

ALOGRITHM	**CREATED BY**	**KEY SIZE(BITS)**	**BLOCK SIZE(BITS)**
DES	IBM IN 1975	56	64
3DES	IBM IN 1978	112 OR 168	64
RIJNDAEL	JOAN DAEMEN & VINCENT RIJMEN IN 1998	256	128
BLOWFISH	BRUCE SCHNEIER IN 1993	32-448	64

Table. 1: Comparison of Various Algorithms [6]

E. A New Image Encryption Approach using The Integration of A Shifting Technique and The AES Algorithm

This paper presented a new image encryption technique is based on the integration of shifted image blocks and basic AES algorithm. In the shifted algorithm technique, the image is divided into blocks. To produce a shifted image, blocks which contain number of pixels are shuffled by using a shift technique that moves the rows and columns of the original image. In AES algorithm, the shifted image is used as an input image to encrypt the pixels of the shifted image. The proposed technique were measured various tests to measure performance. These tests contain histogram analysis, information entropy, correlation analysis, differential analysis. Experimental results showed that the new integration technique has satisfactory security and is more efficient compared to the AES algorithm alone without the shifting algorithm. The results showed that the histogram of an encrypted image produced a uniform distribution, which is very different from the histogram of the plain image, and provide low correlation among image pixels and a high entropy[2] .

F. A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement

Proposed image encryption method consists of two steps. In first step, pixel is rearranged within image using sorting method and in second step image is encrypted using inter-pixel displacement algorithm. All the pixels of image are first stored in an array and then sorting is applied for the pixel rearrangement. The aim behind sorting was reducing the correlation between pixel values. This paper presented a new algorithm for image encryption by using sorting of pixels as per their RGB values and arranging them group-wise which results in low correlation between pixels and high entropy value. Experimental results were taken out on Matlab 6.0.1 and this is a lossless image encryption algorithm with results. Histogram of plain image and cipher image is also carried out[1] .

G. Image Encryption and Decryption Using Image Gradient Technique

This paper presented a new algorithms developed for varying intensity of each pixel and for swapping pixel values within an image. The numeric values used for above encryption called as 'key' is shared as secret key between sender and receiver which are in turn encrypted as images while transmitting ,which is a unique factor in this paper. This paper tries to bring about the fact that by simple manipulation of pixel color values(gradient) and not using external images for this methodology stands as a unique factor. This paper provides a secret key cryptography(SKC) method. In SKC, a single key is used for both encryption and decryption. Sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for encryption and decryption, SKC is known as symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; In SKC, a different approach is used to share secret key between sender and receiver, that is through encryption of numerical secret key into an image which is difficult to detect. The procedure of encryption and decryption implemented in this paper is considered to be having better security rather than other SKC methods, since we encrypt the image in two levels and secret key is encrypted into an image which is unique kind of data to image transformation concept put forward in this paper non-existent in other cryptographic methods. In other visual cryptography or cryptography methods, the final output, though obtained correctly, is not clear enough[1]. This is one of the main drawbacks of other methods. But in this paper, regardless of ample number of manipulations done on a pixel value we get the original image back with same pixel color value which was fed as input to algorithms. This is possible because we apply simple mathematics for manipulations. The application of this cryptographic method can be exercised in the following way. This can be applied in an environment where a group of people need to know the secret information at a time as in a corporate office[7] .

H. An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography

Digital Signature schemes are mostly used in cryptographic protocols to provide services like entity authentication, authenticated key transport and authenticated key agreement. This architecture is related with Secure Hash Function and 512-bit SRNN cryptographic algorithm. SRNN algorithm is based on RSA algorithm with some modification and included more security. In this algorithm we have an extremely large number that has two prime factors (similar to RSA). In addition of this we have used two natural numbers in pair of keys (public, private). This natural number increases the security of the cryptosystem. If the security of our method proves to be adequate, it permits secure communication to be established without the use of carriers to carry keys. In this paper, a new algorithm has been designed for generating signature that overcomes the shortcomings of the RSA system (longer processing time & computational overheads), also the new algorithm can be achieves high security for digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. Basically a Digital Signature is a checksum which depends on the time period during which it was produced. It depends on all the bits of a transmitted message, and also on a secret key, but which can be checked without knowledge of the secret key. A major difference between handwritten and digital signatures is that a digital signature cannot be a constant; it must be a function of the document that it signs. A digital signature algorithm authenticates the integrity of the signed data and the identity of the signatory. A digital signature can be used as an evidence by a recipient of signed data in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. The SRNN algorithm is used for digital signature scheme with 512-bit SRNN algorithm behalf of this algorithm we can secure the communication channel for sender and recipient. We can further use this algorithm for (1024-bit) SRNN algorithm. In this proposed algorithm and proposed signature generation, verification is more secure than RSA algorithm but little slower in speed[8] .

I. New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique

This paper presented a new image encryption algorithm named “New Image Encryption Technique based on Combination of Block Displacement and Block Cipher Technique”. This will provide authorization of users, integrity and safety of images which is traveling over internet. Moreover, an image-based data requires more effort during encryption and decryption. This research introduces an image encryption algorithm which is the combination of “block displacement” and “Block Cipher. The original image was divided into blocks, which is then displaced horizontally and vertically and then resultant image will be divided into pixel blocks. This pixel block will be converted into binary value. Similarly key value will be selected. This key value will be converted in binary form. Finally key value will be XORed with Image value through proposed block based algorithm. Now finally encrypted image will be obtained. The Proposed Algorithm for encryption and decryption of an image using suitable user-defined key is developed. The cipher image generated by this method can vary in size with the original image due to image scaling to make 128 bits block at a time and is suitable for practical use in the secure transmission of confidential information over the Internet. This paper proposed a new image encryption algorithm. It is already known that security of the algorithm is depended on the length of the key that mean longer key length will always support to good security feature and proposed algorithm used 128 bits key length which is provided too much security for the proposed algorithm. To access original key or crypto analysis of the proposed key is required 2128 time to break the key which is almost impossible for any hacker. There is no chance to generate floating point error because no such types of mathematical formula have applied on the proposed algorithm. The correlation co-efficient as well as their entropy values for the proposed algorithm was calculated [9] .

III. CONCLUSION

The security of the data is very important in wireless world since the communication by transmitting of digital data over the network occur very frequently. This paper has been surveyed the existing encryption techniques. Each technique is unique in its own way, which might be suitable for different applications. Some paper provides comparison tables. The implementation of the encryption method will be done using MATLAB. Each encryption techniques have its own advantages and disadvantages.

REFERENCES

[1] Amnesh Goel, Nidhi Chandra “A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement” I.J. Image, Graphics and Signal Processing, 2012, 2, 16-22 Published Online March 2012 in MECS.

[2] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari, Hamida Almangush “A New Image Encryption Approach using The Integration of A Shifting Technique and The Aes Algorithm ” International Journal of Computer Applications (0975 – 8887) Volume 42– No.9, March 2012.

[3] Quist-Aphetsi Kester” A CRYPTOGRAPHIC IMAGE ENCRYPTION TECHNIQUE FOR FACIAL-BLURRING OF IMAGES” International Journal of Advanced Technology & Engineering Research Volume 3, Issue 3, May 2013.

[4] Quist-Aphetsi Kester, “A Visual Cryptographic Encryption Technique for Securing Medical Images” International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2013.

[5] Vidit Pratap Singh, Prof. Dr. Rizwan Beg, Brajesh Mishra,” Practical Approach on Image Encryption and Decryption Technique Using Matrix Transformation**”,** *MIT International Journal of Computer Science & Information Technology Vol. 3, No. 1, Jan. 2013.*

[6] Pia Singh , Prof. Karamjeet Singh,” IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB”, International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[7] Shetty Deepesh Sadananda1, Anusha Karkala2,”Image Encryption and Decryption Using Image Gradient Technique”, Volume 3, Issue 1, January 2013.

[8] Mr. Hemant Kumar, Dr. Ajit Singh,”An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography”, Volume-1 Issue-1, June 2012.

[9] Keerti Kushwah, Sini Shibu.” New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique”, International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013.

[10] Ephin M, Judy Ann Joy, N. A. Vasanthi,” Survey of Chaos based Image Encryption and Decryption Techniques” International Journal of Computer Applications.

[11] Komal D Patel, Sonal Belani,” Image Encryption Using Different Techniques:A Review”,International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 1, November 2011.