A Comprehensive Review on Image Encryption Techniques

Amnesh Goel[1], Dr. Rakesh K Bhujade[2]

[1]*PhD Research Scholar,* [2]*PhD Supervisor*

Department of Computer Science and Engineering, Mandsaur University, Mandsaur, MP 458001, India

Abstract: ***Image encryption methods play a major role in the security and authentication of digital images in multimedia applications. This paper provides a detailed analysis of the various methods of image encryption. This paper covers the most important advances in meta-heuristic imaging-based encryption techniques. Various attacks and accuracy tests related to imaging encryption methods have also been studied. Current methods are studied in terms of differential, predictive and primary evaluations. The main aim of this paper is to provide a general perspective on the characteristics of imaging encryption techniques. The paper begins by reviewing recent advances in image encryption and outlining potential problems.***

Keywords: Image Encryption, Image security, pixel encryption, data loss etc.

I. INTRODUCTION

Due to certain inherent features of the picture, such as low cost and high availability, the use of the networking network has increased and is becoming a cause for the exponential growth of the Internet in the digital world today. Digital photographs play a more important role in our culture than conventional texts and need serious protection of the privacy of users for all applications. The protection of digital images has therefore become more critical and drawn a great deal of interest. Digital image protection can be accomplished using digital image encryption technology. Basically, Image Encryption ensures that the image is converted to an unreadable format such that it cannot be interpreted by third parties. Many data resources need secure protection for the storing and dissemination of digital images[1].Encryption methods for digital photographs play a very important role in preventing unauthorized access to the file.

As digital images are shared through different forms of networks and a major portion of this digital content is either classified or private. Encryption is thus the favored method of securing the transmission of documents. Various security schemes are in use to encrypt and decrypt picture details. But there is no single encryption algorithm that satisfies the various image types[2].

In general, most of the conventional encryption algorithms used are used for text files. While we can use the standard encryption algorithm to encrypt photos directly, this might not be a smart idea for any purpose. First, image data has their unique properties, such as high redundancy and high pixel correlation. Second, they are normally large in scale, making standard encryption techniques impossible to implement and sluggish to process. Third, the decrypted content must be the same as the initial text, although this criterion is not sufficient for image data, because a decrypted image containing a slight distortion is normally appropriate as a feature of human insight. Therefore, algorithms that are ideal for textual data cannot be optimal for multimedia data, While the Triple Data Encryption Standard (T-DES) and the International Data Encryption Algorithm (IDEA) will achieve high security, they may not be appropriate for multimedia applications. As a result, well-known encryption algorithms such as the Data Encryption Standard (DES), the Advanced Encryption Standard (AES) and the International Data Encryption Standard (IDEA) have been developed for text data not for multimedia data[3-4].

Due to advancements in distributed computing networks, recording systems and imaging technologies, digital images have been widely used in different fields [5]. When photos are sent over public networks, they are vulnerable to multiple security attacks, such as eavesdropping, unauthorized modification, replication, etc. As a result, protecting the picture in an effective manner has gained a great deal of coverage in the last few years. The security scheme is split into two parts: information hiding strategies and cryptography. Data hiding methods are further broken down into watermarking and steganography.

Now, let us first understand the Image Encryption process which is base of all this work. Image encryption process basically takes plain image as input and runs the image encryption algorithm on top of that. Image encryption process possesses a key which helps to encrypt the image. Image decryption process is a reverse process of encryption process and outcome of this process produces the plain image back.

Second section of this paper lists out analysis of image encryption techniques. Third section summarize the overall findings based on review of image encryption techniques and concludes the work.

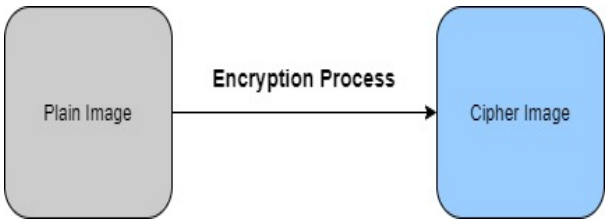

Fig 1: Image encryption process

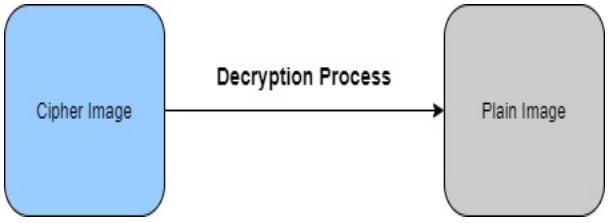

Fig 2: Image decryption process

II. LITERATURE REVIEW

Here is the review of few image encryption algorithms that were proposed lately.

This algorithm improves the accuracy of image encryption compared to the previous one. This algorithm is time-consuming and a dangerous operation. Second, in image encryption using a block-based transformation algorithm, 2008 is based on a combination of image transformation and a well-known encryption and decryption algorithm called blowfish. The original image separated into blocks, which were re-arranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. And the result revealed that the interaction between image elements had decreased significantly. Their finding also shows that increasing the number of blocks by using smaller block sizes has resulted in lower correlation and higher entropy. There is no main generator in this algorithm. Here we use the Blowfish algorithm, which divides the image into several blocks. Due to massive data size and time constraints, an algorithm that is ideal for textual data might not be optimal for multimedia data.

It has got a higher entropy. It has the potential to lose image data for the length of the blockage of the image. It is a lower correlation. Next is image encryption using Hill Cipher's self-invertible key matrix, 2008 which introduces an image encryption technique using the Hill Cipher. They generate a self-invertible matrix for a hill cypher algorithm. Using this main matrix, both the grey scale and the colour picture have been encrypted except for the image with the same gray-level backdrop or the same color[6].

This is an algorithm built on a matrix. It encrypts the grey scale explicitly. It is easy to execute. This algorithm cannot operate on an image with a backdrop of the same grey level or colour. Another survey is an approach to picture encryption using a variation of a permutation strategy followed by encryption. 2008 is approaching a new permutation strategy based on a combination of image permutation and a well-known encryption algorithm called RaijnDael. The original image was divided into four pixel blocks, which were rearranged into a permuted image using a permutation technique, and the produced image was encrypted using the RijnDael algorithm. The findings revealed that the association between image components was greatly reduced with the use of the mixture technique and higher entropy was obtained. It is giving the higher entropy. The association between picture elements is decreased in this process. Here, the method of image permutation was very difficult. The method is often time-consuming, and the chances of error are greater[7].

In 2013, authors [8] suggested a new strategy that would add to the general body of information in the field of cryptography by creating a new cypher algorithm for m*n size picture encryption by shuffling RGB pixel values. With the support of RGB pixels, this algorithm finally encrypts and decrypts the photos. The algorithm has been implemented using MATLAB. In this approach, neither the pixel bit values nor the pixel expansion at the end of the encryption and decryption process are affected. Instead of transposing the numerical values, they are reshaped and concatenated with the RGB values, they are moved away from their respective positions and the RGB values are exchanged to obtain the cypher picture. This shows that the cumulative change of the number of all values in the picture is zero. There is also no difference in the overall size of the picture during the encryption and decryption process. The advantage of their approach is that the signature sizes of the image will remain constant when the encryption process is underway.

In 2012, authors [9] proposed a random scrambling algorithm based on bit-plane image decomposition. Their Algorithm begins by decomposing a grey image into a bit-plane image, each image becoming a bit-plane image. In the next step, every bit of a plane picture is shuffled using a random scrambling algorithm. At last, all the flat bit shuffled images are merged to their original levels on bit-planes, and we've got an encrypted file. Experimental findings suggest that the proposed algorithm successfully scrambled the image as well as seemingly modified the histogram. It has better performance and characteristics than the general random scrambling process. It thus has a more robust scrambling degree than the classical approach Arnold transforms.

This technique has been suggested by Mohammad Ali, Bani Younes and Aman Jantan [10]. In this method, the transformation procedure operates as follows: the original image is separated into a random number of blocks. Ses blocks are then shuffled within the graphic. The created (or transformed) image is then fed into a Blowfish encryption

algorithm. The intelligible details present in the picture is due to the similarity between the elements of the image in the arrangement. As a result, this approach reduced the similarity between the image components using those transformation techniques. The hidden key to this method is used to decide the seed. Seed plays a key role in constructing a transformation table, which is then used to create a transformed image from a different random number of block sizes. The transformation method refers to the procedure of separating and replacing the original image.

Authors[11] suggested a new encryption strategy based on the combination of shift image blocks and simple AES, where the shifted algorithm is used to separate the image into blocks. Each block consists of several pixels, and these blocks are shuffled by a shifting process that moves the rows and columns of the original image in such a way as to create a shifted image. The shifted image is then used as an input image to the AES algorithm to encrypt the pixels of the shifted image. The key theory is that the image can be encrypted by moving the rows and columns of the original image, not by changing the location of the blocks, but by shifting all rows several times based on the shift table, and then the same number of times for the columns for the block layout.

Blood-Su Lee [12] Proposed a system for visual cryptography that uses phase masks and an interferometer. To encrypt a binary file, we divided it into an arbitrary number of slides and encrypted it using an XOR process with a random key or key. The phase mask for each encrypted image was manufactured under the proposed phase assignment law. Phase masks have been mounted on every direction of the Mach-Zehnder interferometer for decryption. Via optical experimentation, we have established that a hidden binary picture that has been sliced can be retrieved using the proposed procedure.

This suggested a new algorithm[13] for the encryption of colour images using chaotic map and spatial bit-level permutation (SBLP). First, use the Logistic Chaotic Series to change the location of the image pixels, then convert it into a binary matrix, and permute the bit-level matrix by scrambling the SBLP-generated mapping. Then use another Logistic chaotic sequence to re-arrange the location of the current image pixels. Experimental findings show that the proposed algorithm can provide strong encryption results and low time complexity, making it ideal for securing video monitoring networks, multimedia devices and real-time applications such as cell phone services.

In this article, authors[14] suggested an advanced Hill (AdvHill) cypher algorithm that uses an Involutory Key Matrix for encryption. The purpose of this paper is to solve the downside of using a random key matrix in Hill's encryption cypher algorithm, where we will not be able to decode the encrypted message if the key matrix is not invertible. Divide the image into blocks by applying the involuntary key matrix to each block and creating a temporary block using the ith pixel value of each block again by multiplying it with the involuntary key matrix and transposing it to the endpoint.

III. CONCLUSION

This paper includes an exhaustive analysis of the latest strategies for encrypting images. This paper classifies the current strategies of image encryption in a succinct and efficient manner. It has been noted that security bugs, parameters tuning, and computational speed are still an open area of study in the field of image encryption. Various researchers have designed meta-heuristic-based imaging techniques to address these concerns. Most current meta-heuristic imaging techniques also suffer from low convergence speed, premature convergence, and local optimization. The issues and potential opportunities for study related to imaging encryption strategies have been addressed. From a thorough analysis of current imaging encryption methods, it has been concluded that imaging encryption is still an underdeveloped area. It is largely unexplored in numerous imaging technologies such as subwater, remote sensing, multi-spectral imaging, and 3D imaging systems.

REFERENCES

[1] I. Öztürk and I. Sogukpınar, "Analysis and comparison of image encryption algorithms", Transactions on Engineering, Computing and Technology, vol. 3, pp. 1305-5313, 2004.

[2] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[3] V. Potdar and E. Chang, "Disguising text cryptography using image cryptography", International Network Conference in Plymouth, UK, 6 - 9 July, 2004.

[4] X. Li, J. Knipe, and H. Cheng, ," Image Compression and Encryption Using Tree Structures" , Pattern Recognition Letters, Vol. 18, No. 8, pp. 2439 2451, 1997.

[5] Ghebleh M, Kanso A, Noura H (2014) An image encryption scheme based on irregularly decimated chaotic maps. Signal Process Image Commun 29(5):618–627

[6] M.aliBani, younes, and a.jantan, Image Encryption using block based Transformation Algorithm 2008.

[7] S.P.Nanavati, P.K. Panigrahi. "Wavelets: applications to image compression-I," Joined of the scientific and engineering computing, vol.9, no.3, 2004, pp.4-10.

[8] Quist-Aphetsi Kester," A cryptographic Image Encryption technique based on the RGB PIXEL shuffling", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, January 2013.

[9] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma," Image Encryption Based on Bit-plane Decomposition and Random Scrambling", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012.

[10] Mohammad Ali, Bani Younes and Aman Jantan,"Image Encryption Using BlockBasedTransformation Algorithm".

[11] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush. "A New Image Encryption Approach using the Integration of a Shifting Technique and the AES Algorithm". International Journal of Computer Applications. March 2012

[12] Sang-Su Lee, Jung-Chan Na, Sung-Won Sohn, Cheehang Park, "Visual Cryptography Based on an Interferometric Encryption Technique", ETRI Journal, Volume 24, Number 5, October 2002 pp. 373-380.

[13] Kuldeep Singh, Komalpreet Kaur, Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it, International Journal of Computer Applications (0975 –8887) Volume 23– No.6, June 2011.

[14] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self Invertible Key Matrix of Hill Cipher Algorithm, 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.