A Review on Image Encryption Technique and to Extract Feature from Image

Samridhi Singh
PG Student
Department of
Information Technology,
College of Technology
G.B.P.U.A&T,Pantnagar,
Uttrakhand,India

H. L. Mandoria
Professor
Department of
Information Technology,
College of Technology
G.B.P.U.A&T,Pantnagar,
Uttrakhand,India

ABSTRACT
The security of image data from unauthorized users is important hence image encryption play an important role in hiding information. This survey paper measure up the different encryption techniques for securing multimedia data with objective to give complete review on the various encryption techniques. This paper presents a review of survey literature published from 2008 to 2015 in aspect of different image encryption/decryption techniques with tabular form and the algorithms used to extract the features from the images.

Keywords
Encryption, feature extraction, color, texture, algorithms.the correlation between image elements was significantly decreased. Results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy [1].

An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption: It is a new permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael. The original image was divided into 4×4 pixels blocks, which were repositioned into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm [2]. Younes results show that the connection between image elements was significantly decreased by using the combination technique and higher entropy was attained.

1. INTRODUCTION
Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. The art of protecting information by transforming it (encrypting) into an unreadable format, called cipher text. Only those who obtain a secret key can decipher (or decrypt) the message into plain text, this process is called cryptography. Encrypted data can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually indestructible. To encrypt the image for the transmission over unsecured channels image pattern is decided by the key which is used for encryption and that pattern is decided on the basis of key which is generated after extracted features of the image.

Nowadays when more defensive information is stored on computers and transmitted over unsecured channel, it needs to fortify information security. Image is also an important part of information. Therefore it‟s very important to protect image from unauthorized access. There are so many algorithms available to protect image from unauthorized access which is described below:

Image Encryption Using Block-Based Transformation: Block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were reshuffled into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. Younes results showed that

Image Encryption Using Affine Transform and XOR Operation: It‟s a two phase encryption and decryption algorithms that is based on rearranging the image pixels using affine transform and encrypting the resulting image using XOR operation. Redistribute the pixel values to different location using affine transform technique with four 8-bit keys. The transformed image then divided into 2 x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys [3]. The total key size used in algorithm is 64 bit. Amitava Nag results proved that after the affine transform the relations between pixel values was significantly decreased.

Image Security via Genetic Algorithm*:* In this technique, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are applied as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image [4].

Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps: Kotal presented multiple chaotic maps based on a new symmetric image encryption algorithm. In the proposed algorithm, with the help of general Arnold Cat Map, the plain image is first scrambled. Further, the scrambled image at a particular iteration is encrypted using chaotic sequences generated by one dimensional Logistic Map after preprocessing them to

integers. The results demonstrate that the grayscale images can be successfully encrypt and decrypt with secret keys by proposed algorithm. It also present that the proposed method is secure, loss-less, and resourceful [5].

Image Encryption and Decryption Using Blowfish Algorithm in Matlab*:* Encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish [6] is considered to increase security and to improve performance. This algorithm is used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular accessible algorithms.

The proposed algorithm is designed and realized using MATLAB. Hence if the number of rounds is increased then the blowfish algorithm becomes stronger. Since Blowfish does not have any known security weak points so far it can be considered as an excellent standard encryption algorithm.

A Keyless approach to Lossless Image Encryption: In this method [7] an improved Keyless approach for image Encryption in lossless RGB images is used there are three different approaches being followed in image encryption: key oriented encryption, Image splitting and multiple share. This approach increase the security level and to improve the storage capacity with SST techniques. The security level was increased by randomly distributing the pixel bit over the entire image. Using keyless approach, without any loss of quality reversible encryption would be done and to maintain the originality of an image.

Image Encryption using CAT Mapping and Chaos Approach*:* An innovative method which uses Cat mapping to realize the image discretization. This approach uses the periodic changes to achieve the encryption of images. Images with different sizes may use different cycles to encrypt. This encryption approach is able to fulfill the image encryption effectively through drawing the best parameters to achieve the best image encryption effect. The sensitivity analysis implies that, this method is capable of performing well on the image pixel scrambling and replacement. For encrypted security, this method has strong sensitivity to the

plaintext which may attribute to handle the plaintext attack under difference situations [8].

An Ethical Approach of Block Based Image Encryption Using Chaotic Map*:* In this algorithm two dimensional chaotic map and the two secrets keys for encryption of an image were used in which first the image was divided into four blocks and then each block of the image was encrypted individually in n times, after that the keys are inverted for each block and the process was repeated up to m times. The work can be rigorously examined over the prevalent standard test like key sensitivity analysis, statistical analysis, differential analysis, entropy analysis, which make the proposed algorithm good enough for real time secure communication.

A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps*:* An image encryption technique using DNA (Deoxyribonucleic acid) operations and chaotic maps [9]. Firstly, the input image is DNA encoded and a mask is generated by using 1D chaotic map. Secondly, this mask is added with the DNA encoded image using DNA addition. The intermediate result is DNA complemented with the help of a complement matrix produced by two 1D chaotic maps. Finally, the resultant matrix is permuted using 2D chaotic maps followed by DNA decoding to get the cipher image. This technique is totally invertible and it can resist known plain text attacks, statistical attacks and differential attacks.

Review on DES, AES and Blowfish for Image Encryption & Decryption*:* In this paper on DES, AES and Blowfish for Image Encryption and Decryption are discussed [10]. In this era it is a crucial concern that while transferring image from one network to another over the internet, the proper encryption and decryption should be applied so that unauthorized access can be prevented.

Table1. Comparison of Different Encryption method

Encryption Technique	Author name, Year	Method used	Result
Image Encryption Using Block-Based Transformation[1]	Mohammad Ali Bani Younes and Aman Jantan, 2008	The proposed technique showed that an inverse relationship exists between number of blocks, and a direct relationship between number of blocks and entropy.	The proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy.
An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption[2]	Mohammad Ali Bani Younes, 2008	Introduce a new permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael	This method enhances the security level of the encrypted images by dropping the correlation among image elements, increasing its entropy value by decreasing the mutual information among the encrypted image variables
Image Encryption Using Affine Transform and XOR Operation[3]	Amitava Nag, 2011	Reorganize the pixel values to different location using affine transform technique distorted image is then encrypted using XOR operation.	Improved Solution and Correlation between pixels values drastically increases.
Image Security via Genetic Algorithm[4]	Rasul Enayatifar and Abdul Hanan Abdullah, 2011	The chaotic function is in use for initial encryption and the genetic algorithm is used to improve the encryption process of the image	First time genetic algorithm is used to encrypt the image and in result it proves highly efficient compared with other method.
Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps[5]	S. Som, A. Kota, 2012	The plain image is first scrambled using generalized Arnold Cat Map. Further, the scrambled image at a particular iteration is encrypted using chaotic sequences	The study prove the security, effectiveness and robustness of the proposed image encryption algorithm

		generated by one-dimensional Logistic Map.	
Image Encryption And Decryption Using Blowfish Algorithm In Matlab[6]	Pia Singh, 2013	Encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times.	Blowfish cannot be broken until an attacker tries 28r+1 combinations where r is the number of rounds. Hence if the number of rounds are been increased then the blowfish algorithm becomes stronger.
A Keyless approach to Lossless Image Encryption[7]	Pratibha S. Ghode, 2014	Three different approaches being followed in image encryption, the first approach to key oriented encryption and second approach to Image splitting and the final approach multiple shares.	Proposed encryption algorithm can ensure the lossless of transmissions of images and increase the security level and decrease the CPU computational time.
Image Encryption using CAT Mapping and Chaos Approach[8]	Weihua zhu, 2014	By using cat mapping the pixel value from image is scrambled then the pixel value is replaced by a new hybrid chaotic system and the proposed method enhances the ability of the algorithm to resist select plaintext attack.	Ideal for image encryption under the situation of a large amount of data and real time requirement.
An Ethical Approach of Block Based Image Encryption Using Chaotic Map[9]	Kamlesh Gupta, Ranu Gupta, 2015	In the proposed algorithm two dimensional chaotic map and two secrets keys for encryption of image are used in which first divide the image into four blocks and then each block of the image is encrypted independently in n times, after that the keys are reversed for each block and repeat times	The proposed method is predicted to be useful for real time image encryption and transmission applications.
A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps[10]	Anchal Jain · Navin Rajpal, 2015	The input image is DNA encoded and a mask is generated by using 1D chaotic map. This mask is added with the DNA encoded image using DNA addition. Intermediate result is DNA complemented with the help of a complement matrix produced by two 1D chaotic map	It is robust to various attacks like known plain text attack, statistical attacks and differential attacks

2. IMAGE FEATURE EXTRACTION TECHNIQUES

Feature extraction is one of the most significant fields in artificial intelligence. It consists to extract the most appropriate features of an image and assign it into a label. In image classification, the crucial step is to evaluate the properties of image features and to organize the statistical features into classes.

2.1 Color Features

In image classification and image retrieval, the color is the most significant feature. The color histogram describes the most frequent method to extract color feature. It is regarded as the distribution of the color in the image [20]. The efficiency of the color feature resides in the fact that is independent and insensitive to size, rotation and the zoom of the image.

2.2 Texture Features

Texture feature extraction is very robust method for a large image which contains a recurring region. The texture is a group of pixel that has certain characterize. The texture feature methods are classified into two categories: spatial texture feature extraction and spectral texture feature extraction [19].

2.3 Shape Features

Shape features are used in the literature (in object recognition and shape description). The shape features extraction techniques are classified as: region based and contour based [18]. The contour methods calculate the feature from the boundary and disregard its interior, while the region methods calculate the feature from the entire region. Feature detection and image matching represent two important tasks in all images applications. The selection of adequate method to complete a matching task significantly depends on the type [22] of image to be matched and in the variations within an image and its matching pair in one or many of the following parameters:

a) Scale: At least two elements of the set of images views have different scales.

b) Occlusion: Is the concept that two objects that are spatially separated in the 3D world might interfere with each other in the projected 2D image plane.

c) Orientation: The images views are rotated with respect to each other.

d) Affine Transformation: Equally distorted image can correct for a range of perspective distortions.

e) Blurring: It is the apparent streaking of rapidly moving objects in a still image or a sequence of images.

f) Illumination: Changes in illumination also represent a typical problem for accurate feature matching

3. OVERVIEW OF IMAGE FEATURE EXTRACTION ALGORITHMS

3.1. Feature-based algorithm

3.1.1. Color histogram (color detector)

A color histogram is a representation of the distribution of colors in an image [13]. For digital images, a color histogram represents the number of pixels that have colors in each of a fixed list of color ranges that span the image‟s color space, the

set of all possible colors. The main problem of histograms for classification is that the representation is reliant of the color of the object being studied, ignoring its shape and texture. Color histograms can potentially be identical for two images with different object content which happens to share color information.

3.1.2. FAST (corner detector)

FAST (Features from Accelerated Segment Test) algorithm With FAST, the detection of corners was prioritized over edges as they claimed that corners are one of the most intuitive types of features that show a strong two dimensional intensity change, and are therefore well distinguished from the neighboring points [21]. The feature-based detectors only perform accurately when the objects to be matched have a same color or a distinguishable corner or edge. Furthermore, the feature-based algorithms do not perform as good as expected when images are subjected to variations in color‟s distribution, scale, illumination, rotation or affine transform. To overcome these limitations, a new class of image matching algorithm was developed simultaneously. These algorithms are known as texture-based algorithms because of their capability to match features between different images despite of the presence of textured backgrounds and lack of planar and well-defined edges.

3.2. Texture-based algorithm

3.2.1. SIFT detector

SIFT (the Scale Invariant Feature Transform) for extracting distinctive invariant features from images that can be invariant to image scale and rotation [14]. Then it was widely used in image mosaic, recognition, retrieval and etc.

3.2.2. PCA-SIFT detector

PCA-SIFT (Principal Component Analysis-SIFT) is a standard technique and new algorithm emerged as an attempt to improve SIFT, for dimensionality reduction and eliminate the computational costs. PCA (Principal Component Analysis-SIFT) to normalize gradient patch instead of histograms. Authors showed that PCA-based local descriptors were also distinctive and robust to image deformations

3.2.3. SURF detector

The Speed-Up Robust Feature detector (SURF) was conceived to ensure high speed in three of the feature detection steps: detection, description and matching. Unlike PCA-SIFT, SURF speeded up the SIFT detection process without scarifying the quality of the detected points. SIFT and SURF algorithms employ slightly different ways of detecting features. SIFT builds an image pyramids, filtering each layer with Gaussians of increasing sigma values and taking the difference. On the other hand, SURF creates a stack without 2:1 down sampling for higher levels in the pyramid resulting in images of the same resolution.

3.2.4. F-SIFT detector

F-SIFT (Fast-SIFT) consists of the same four major stages of SIFT: (a) scale-space detection, (b) key point localization, (c) orientation assignment and (d) key point descriptor and feature vector is significantly smaller than the standard SIFT feature vector.

Table2. Conclusion of entire above algorithm

Method	Timing	Transformation	Scaling	Rotation	Blurring	Illumination
FAST	Common	Common	Common	Bad	Bad	Bad
SIFT	Bad	Good	Good	Best	Best	Best
PCA-SIFT	Good	Bad	Bad	Common	Common	Bad
F-SIFT	Best	Good	Best	Good	Good	Good
SURF	Good	Best	Best	Good	Good	Good

4. CONCLUSION

Cryptography is very significant to provide security against statistical attacks and other types of attacks when images are exchanged between two parties on the network. This paper presents a review of survey literature of different image encryption/decryption techniques with tabular form and concluded that all techniques are high-quality for image encryption and have their own advantages and disadvantages and give a protection so that no one can have right to use the image which is in the open network and also in this paper evaluated five feature detection methods for image deformation. It was concluded that F-SIFT has the best overall performance above SIFT and SURF but it suffers from detecting very few features and therefore

matches. It is suggested that the properties of this algorithm to be improved by creating a new implementation provided with a matching component. Future research in this area should focus on testing the precision of the algorithms in detecting a single object within a picture. And, also improve semantic techniques with F-SIFT extraction feature algorithm to eradicate semantic gap between high-level semantic perception of person and low-level features of an image.

5. REFERENCES

[1]. Mohammad Ali Bani Younes et al (2008) "Image Encryption Using Block-Based Transformation Algorithm" IAENG International Journal of Computer Science.

[2]. Mohammad Ali Bani Younes et al(April 2008), "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption", IJCSNS International Journal of Computer Science and Network Security

[3]. Amitava Nag et al (2011)"Image Encryption Using Affine Transform and XOR Operation", InternationalConference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN).

[4]. Rasul Enayatifar et al(2011)" Image Security via Genetic Algorithm", International Conference on Computer and Software Modeling IPCSIT vol.14

[5]. Sukalyan Som et al (2012)" Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps", National Conference on Computing and Communication Systems (NCCCS).

[6]. Pia Singh et al (July-2013) "Image Encryption and Decryption Using Blowfish Algorithm in Matlab," International Journal of Scientific & Engineering Research, vol. 4, Issue. 7.

[7]. P. S. Ghode, (May 2014) "A Keyless approach to Lossless Image Encryption", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE.), vol. 4, Issue. 5, pp. 1459- 1467.

[8]. W. Zhu, (2014) "Image Encryption using CAT Mapping and Chaos Approach," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pp.1-8.

[9]. A. Jain et al (February 2015) "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," Multimedia Tools and Applications, An International Journal, Springer Science + Business Media Ne Yourk, pp. 1-18.

[10]. A. Devi et al (2015) "A Review on DES, AES and Blowfish for Image Encryption & Decryption," (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, Issue. 3, pp. 3034-3036. http://www.ijcsit.com.

[11]. Liang Zhao et al (2012) "On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption", Communications in Nonlinear Science and Numerical Simulation, Vol. 17, No. 8, pp3303-3327.

[12]. G.A. Sathishkumar et al (2011) "A novel image encryption algorithm using pixel shuffling and BASE 64 encoding based chaotic block cipher, WSEAS Transactions on Computers, Vol. 10, No. 6, pp169-178.

[13]. Jinxia L et al, "Application of SIFT feature extraction algorithm on the image registration". In: Tenth international conference on electronic measurement & instruments IEEE.

[14]. Lowe D., (2004) "Distinctive image features from scale-invariant key points". IJCV 2004; 60(2):91–110.

[15]. Wang X., "Robust image retrieval based on color histogram of local feature regions". Springer Netherlands; 2009.

[16]. Stokman H et al, (March 2008)" Selection and fusion of color models for image feature detection". Pattern Anal Mach Intel IEEE Trans; 29:371–81.

[17]. Rosen E et al, (2010) "FASTER and better: a machine learning approach to corner detection". IEEE Trans Pattern Anal Mach Intel; 32:105–19.

[18]. D. Zhang et al,(2004) "Review of shape representation and description techniques", Pattern Recognition, vol. 37, no. 1, pp. 1-19.

[19]. L. Li et al, (2012) "Texture Classification from Random Features," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 574-586.

[20]. M. K. Swain et al (1991.) "Color indexing". International Journal of Computer Vision, vol. 7, no. 1, pp. 11-32.

[21]. Rosten E et al (2010) "FASTER and better: a machine learning approach to corner detection". IEEE Trans Pattern Anal Mach Intel; 32:105–19.

[22]. D. P. Tian et al (2013) "A Review on Image Feature Extraction and Representation", Techniques International Journal of Multimedia and Ubiquitous Engineering, vol. 8, no. 4, pp. 385-396.

[23]. Sonal Paliwal et al,(June 2016)"A survey on various Text Detection and Extraction technique from videos and images". IJCSEITR

[24]. Bhomika Pandey et al, "A Comprehensive study on text and image stenography", IJETTCS, February 2016.

[25]. Navneet kr. Kashyap et al, (may 2016)"Analysis of pattern identification using graph database for fraud detection",, OJCST.

[26]. Poonam Singh et al (Sep 2015)" Performance analysis of image and video coding by Wavelet Transform Using Region of interest", IJERMT.

[27]. Dixcha Gusain et al, (January 2016) " Comparative analysis of filters for extraction from noisy images", IJESRT.