# Survey of Various Image Encryption Methods and Evaluation Matrices

Divya Aarushi[#1], Sunil Ahuja[*2]

[#]Research Scholar, Department of Computer Science & Engineering
Doon Valley Institute of Engineering & Technology, Karnal
[*]Assistant Professor, Department of Computer Science & Engineering
Doon Valley Institute of Engineering & Technology, Karnal

***Abstract—*** *In present years, there has been momentous progress in multimedia technologies. Transmission of multimedia data such as audio, video and pictures above the Internet is nowadays extremely common. Though internet is extremely insecure channel and this poses a number of protection issues. To accomplish confidentiality and protection of multimedia data above an insecure channel like the Internet, a number of encryption schemes have been proposed. The existence of multimedia technology in this era has promoted digital images to play a more important role than the traditional texts, which demand serious protection of users' privacy for all applications. However, with the help of various types of networks digital images are exchanged. Sometimes, it is true that a large part of this data is either confidential or private. So, preferred technique for protecting the transmitted data is encryption. There are many systems to encrypt and decrypt image data for security. This paper surveys some of Image Encryption methods and evaluation Metrics.*

***Keywords:*** *Image Encryption, RSA Encryption, Chaotic Map*

## I. CRYPTOGRAPHY

Cryptography is the science of retaining mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive data or dispatch it across insecure webs (like the Internet) so that it cannot be elucidate by anybody except the aimed recipient. Cryptography is the science of safeguarding data; cryptanalysis is the science of analyzing and obliterating safeguard communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, appeal of mathematical instruments; chart discovering, patience, determination, and luck. Cryptanalysts are additionally yelled attackers. Cryptology embraces both cryptography and cryptanalysis.

Cryptographic strength is measured in the period and resources it must to demand to recoup the plaintext. The consequence of forceful cryptography is cipher text that is incredibly tough to decipher lacking ownership of the appropriate decoding tool. How difficult? Given all of today’s computing manipulation and obtainable time—even a billion computers substituting a billion checks a second—it is not probable to decipher the consequence of forceful cryptography beforehand the finish of the universe. One must to contemplate, consecutive, that forceful cryptography must to grasp up rather well opposite even an incredibly motivated cryptanalyst. Who’s candidly to say? No one has proven that the strongest encryption obtainable nowadays will grasp up below tomorrow’s computing power.

## II. HOW DOES CRYPTOGRAPHY WORK?

A cryptographic algorithm, or cipher, is a mathematical aim utilized in the encryption and decryption process. A cryptographic algorithm works in combination alongside a key—a word, number, or phrase—to encrypt the plaintext. The comparable plaintext encrypts to disparate cipher text alongside disparate keys. The protection of encrypted data is completely reliant on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all probable keys and all the protocols that make it work encompass a cryptosystem. PGP is a cryptosystem.

### *Image Encryption Techniques*

Image encryption is a method that provides protection to pictures by changing early picture to one more picture that is tough to understand. Countless encryption methods are continuing that are utilized to circumvent the data stealing. Picture encryption has requests in internet contact, multimedia arrangements, health imaging, telemedicine, martial contact, etc.

## III. CHAOS BASED IMAGE ENCRYPTION TECHNIQUE

Chaos word has been derived from the Greek, that mentions to unpredictability. Disorder theory is mathematical physics that was industrialized by Edward Lopez. Disorder is suitable for picture encryption, as it is closely connected to a little dynamics of its own characteristics. The deed of the disorder arrangement, below precise conditions, presents phenomena that are described by sensitivities to early conditions and arrangement parameters.

Finished way to chaos-based cipher design consists of four steps:

1. Choosing a chaotic map: one should consider maps with good mixing property, robust chaos, and a large parameter set.
2. Introducing the parameters.
3. Discretization.
4. Cryptanalysis and key scheduling

## IV. RSA BASED IMAGE ENCRYPTION

RSA involves a area key and a confidential key. The area key can be recognized by nodes and is utilized for encrypting messages. Memos encrypted alongside the area key can merely be decrypted in a reasonable number of period employing the confidential key. The keys for the RSA algorithm are generated the pursuing method:

1. Choose two distinct prime numbers *p* and *q*.
2. For security purposes, the integer's *p* and *q* should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
3. Compute *n* = *pq*.
4. *n* is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
5. Compute φ(*n*) = φ(*p*)φ(*q*) = (*p* − 1)(*q* − 1) = *n* - (*p* + *q* -1), where φ is Euler's totient function. This value is kept private.
6. Choose an integer *e* such that 1 < *e* < φ(*n*) and gcd(*e*, φ(*n*)) = 1; i.e., *e* and φ(*n*) are coprime.
7. *e* is released as the public key exponent.
8. *e* having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16}$ + 1 = 65,537. However, much smaller values of *e* (such as 3) have been shown to be less secure in some settings.[5]
9. Determine *d* as $d \equiv e^{-1}$ (mod φ(*n*)); i.e., *d* is the modular multiplicative inverse of *e* (modulo φ(*n*)).
10. This is more clearly stated as: solve for *d* given *d*⋅*e* ≡ 1 (mod φ(*n*))
11. This is often computed using the extended Euclidean algorithm. Using the pseudo code in the *Modular integers* section, inputs *a* and *n* correspond toe and *φ*(n), respectively.
12. *d* is kept as the private key exponent.
13. The *public key* consists of the modulus *n* and the public (or encryption) exponent *e*. The *private key* consists of the modulus *n* and the private (or decryption) exponent *d*, which must be kept secret. *p*, *q*, and φ(*n*) must also be kept secret because they can be used to calculate *d*.

## V. EVALUATION METRICS

### Correlation Coefficient

Statistical scrutiny such as correlation coefficient factor is utilized to compute the connection amid two variables; the picture and its encryption. This factor demonstrates to what extent the counseled encryption algorithm powerfully resists statistical attacks. Therefore, encrypted picture have to be completely disparate from the early one.

If the correlation coefficient equals one, that way the early picture and its encryption is identical. If the correlation coefficient equals zero, that way the encrypted picture is completely disparate from the early (i.e. good encryption). If the correlation coefficient equals minus one that way the encrypted picture is the negative of the early image.

The correlation coefficient is measured by the pursuing equation:

$$C.C = \frac{\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N} (x_i - E(x))^2} \sqrt{\sum_{i=1}^{N} (y_i - E(y))^2}}, \qquad (3)$$

C.C: correlation coefficient

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i, \qquad (4)$$

x and y: gray-scale pixel values of the original and encrypted images.

### Encryption Quality

A measure for encryption quality may be expressed as how much the deviation (changes) caused in pixel values at every location of the plain-image. The following steps summarize this measure:-

1. X =| I − E |
2. H = histogram (X)
3.

$$D = \frac{1}{256} \sum_{i=0}^{255} h_i, \qquad (1)$$

4. S(i) =| H(i) − D |
5.

$$AS = \sum_{i=0}^{255} D(i), \qquad (2)$$

I: the plain-image.
E is the encrypted image.
H: histogram distribution.
$h_i$: the amplitude of the absolute difference histogram at the value i.

The lower value of area 'AS' under the absolute curve 'S', that means the more effective of image encryption and hence the encryption quality.

**Execution Time**

Another vital instrument to assess the efficiency of algorithms is computing the number of period needed to encrypt an image. In this investigation, actual period in CPU cycles will be utilized as a compute of killing time.

3.1.5 Differential Attack

In finish, a desirable property for an encrypted picture is being sensitive to the tiny adjustments in plain-image (e.g., modifying merely one pixel). Antagonist can craft a tiny change in the input picture to discern adjustments in the result. By this method, the meaningful connection amid early picture and encrypted picture can be found. If one tiny change in the plain-image can cause a momentous change in the cipher-image, alongside respect to diffusion and confusion, next the differential attack truly loses its efficiency and becomes usefully useless. Three public measures were utilized for differential analysis: MAE, NPCR and UACI.

MAE is mean absolute error.

NPCR means the number of pixels change rate of ciphered image while one pixel of plain-image is changed.

UACI which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image.

Let *C (i, j)* and *P (i, j)* be the gray level of the pixels at the ith row and jth column of a W×H cipher and plain-image, respectively. The *MAE* between two images is defined as

$MAE=1/W*H \, {}^{W}\sum_{j=1} {}^{H}\sum_{i=1} | c(i,j)-p(i,j)|$

Consider two cipher-images, *C1* and *C2*, whose corresponding plain-images have only one pixel difference. The *NPCR* of these two images is defined in

$NPCR=\sum_{ij} D(i,j)*100\%$

Where *d(i,j)* is defined as 0 or 1.

UACI is defined by the following formula:

$UACI=1/w*H \, (|c_1(i,j)c_2(i,j))|*100)/255$

The larger the MAE value, the better the encryption security. The UACI estimation result shows that the rate influence due to one pixel change.

## VI. RELATED WORK

**Bagheri, M. et al, in "Evolution of mapping functions for image encryption using Evolvable Hardware" 2010 [1],** the authors describe The security of digital images attracts much attention recently. For images the transformation can be implemented at two levels, the first one consists of the pixel value permutation and the second one consists of position permutation. In this paper, they propose an encryption scheme for digital images with new pixel position permutation method based on Evolvable Hardware (EHW). In this work, they use EHW to find an equation for mapping functions for encryption and decryption process. The main contribution of this work is that they can evolve arbitrary mapping functions by using EHW. Therefore, there is no limit in selecting map functions. This method of permutation is very fast and cost effective for implementation on reconfigurable devices like FPGAs.

**Metzler, R.E.L. et al, in "Selective region encryption using a fast shape adaptive transform" 2010 [2],** the authors describe Selective regional encryption was performed on nonrectangular, statistically relevant regions of image media by permutation of coefficients in the domain of a fast, shape adaptive, parametric transform in order to partially encrypt the original image. Regions were successfully segmented using a high order information analysis. A simple encryption scheme which exploits the energy compaction properties of a shape adaptive cosine transform was then applied in the transform domain. Computer simulation shows that the method is fast and statistically secure.

**Seyedzadeh, S.M. et al, in "Using self-adaptive coupled piecewise nonlinear chaotic map for color image encryption scheme" 2011 [3],** the authors describe In recent years, various image encryption algorithms based on chaos-based image cryptosystems have been proposed. In this paper, a design of the compound one-dimensional chaotic function by coupling piecewise nonlinear chaotic map and nearest-neighboring coupled-map lattices (NCML) suggests self-adaptive color image encryption. The coupling and nonlinear structure of the compound chaotic function enhances cryptosystem security. The self-adaptive color image encryption is carried out by using one half of the image data for encryption of the other half of the image recursively. The salient features of the proposed image encryption scheme are high security level, high sensitivity, high speed and large key space. In order to generate the initial conditions and parameters of the chaotic function of one half of the image, 192-bit-long external secret key and the other half of the image data are used. The results of several experimental, statistical analysis and key sensitivity tests for color images have shown the high performance on the sensitivity, speed and security of the proposed algorithm.

**Dan-hua Liu et al, in "A robust image encryption scheme over wireless channels" 2009 [4],** the authors describe In traditional image encryption system, decryption is extremely sensitive to packet loss. However, in wireless networks, packet loss is inevitable. Compressed sensing (CS) theory shows that sparse signal can be recovered from few incomplete measurements of it. Strong randomness of measurement matrix and irrelevance among the elements of the measurement vector imply that measurement process can be regarded as encryption process. So, this paper, based on CS theory, presents a new image encryption scheme with robustness to packet loss. In the scheme, they design a Gaussian random measurement matrix as the key to realize data encryption. Moreover, to enhance the incoherence between the plain-image and the cipher-image, they add a random disturbance term to the measurements (cipher-image) and thus improve the security level of the cipher-image. Numerical experiments show that the proposed method not only has well anti-attack ability but also is robust to packet loss, which can still decrypt plain-image even when the packet loss ratio is up to 50%.

**Nini, B. in "Projection based permutation of color images" 2012 [5],** the authors describe The encryption of images is based on two main complementary techniques: permutation and substitution of pixels. The strength of any encryption algorithm depends on the strength of both techniques. This paper presents an algorithm for rows and columns permutation of pixels. It introduces a virtual cylinder surrounding the image through which a virtual viewer looks at the image when rotating around it. The key idea is based on the fact that the line of sight of each pixel to the viewer intersects the cylinder surface at a given point. This point should be the same whatever the position of the viewer is. Therefore, it is used to find out the new pixel's position corresponding to the original image in a new generated image which is viewed from another position. The new created image has then some pixels which stack up and others which become out. They are then reintroduced in the created holes in the new image. This reinsertion of pixels creates the expected permutation. Based on only two main parts of the key which can be reinforced by others and a substitution technique, the algorithm shows a strength transformation of images for the purpose of their encryption.

**Sajasi, S. et al, in "A high quality image hiding scheme based upon noise visibility function and an optimal chaotic based encryption method" 2013 [6],** the authors describe This paper presents a novel image steganographic approach for hiding a secret image in the cover image deals with improving both visual quality of the stego-image and the security of the secret image, while still providing a large embedding capacity. First, to improve both the visual quality and to keep the embedding capacity at an acceptable level, the payload of each region of the cover image is determined dynamically based on Noise Visibility Function (NVF). Second, to ensure the security of the secret image, an optimal chaotic based encryption method is generalized to transform the secret image into an encrypted image. Third, the optimal chaotic based encryption method is obtained by using GAiPSO algorithm to find an optimal secret key. The optimal secret key is able to encrypt the secret image in such a way that after embedding, the rate of changes in the stego-image can be decreased which result in increasing the quality of the stego-image. The experimental results demonstrate that the proposed scheme is able to achieve a good trade-off between the payload and the setgo-image quality.

**Shang-Lin Hsieh et al, in "A Copyright Protection Scheme for Gray-Level Images Using Human Fingerprint" 2006 [7],** the authors describe This paper proposes a copyright protection scheme using human fingerprint images as watermarks. The scheme includes the feature extraction of the fingerprint image and the generation of the share image used to retrieve the fingerprint image. If an unauthorized copy is found later, the origin of the copy can be determined by the retrieved fingerprint image. Fingerprint image enhancement technique is employed prior to feature extraction to obtain a more reliable estimation of feature locations. In addition, the paper employs correction to reform the quality of the fingerprint image. According to the experimental results, the acceptance rate is up to 99% under several severe conditions. The experimental results also show that the scheme can tolerate several image processing attacks on the host image

**Junling Ren in "Information hiding algorithm for palette images based on HVS" 2010 [8],** the authors describe This article is based on Human Visual System (HVS). The carrier image is divided into three regions: the smooth region, the texture region and the fringe region. After the secret image being scrambled, the different merging coefficients are set in the respective region of the carrier image to mix the secret image and the carrier image together. According to the characteristics of the palette image, the scrambling coefficients are embedded into the carrier image palette to increase the confidentiality of the information. During carrier image partitioning, variation coefficient is introduced to describe the data dispersion degree of the image. Thus the stability of the threshold is enhanced, and a much better hiding effect on the secret information is achieved.

**Lukac, R. et al, in "Digital image indexing using secret sharing schemes: a unified framework for single-sensor consumer electronics" 2005 [9],** the authors describe This paper introduces a color filter array (CFA) image indexing approach for cost-effective consumer electronics with image capturing capability. Using a secret sharing technique, the proposed method indexes captured images directly in the single sensor digital camera, mobile phone and pocket device by embedding metadata information in the CFA domain. The metadata are used to determine ownership, capturing device identification numbers, and to provide time and location information. Additional semantic information could be added in the metadata by the end-user through the mobile phone's or pocket device's keyboard. After the metadata are embedded to the CFA image, the subsequent demosaicking step reconstructs a full color RGB image with excellent visual quality. The metadata information can be extracted from the CFA images. Alternatively, it can be recovered by the demosaicked images in personal image databases using PC software commonly available by camera manufacturers or with conventional public image database tools. The uniqueness and efficiency of the proposed approach are demonstrated here by employing a common Bayer CFA based imaging pipeline, however, the approach is suitable for other, non-Bayer CFA patterns, as well.

**Saini, J.K. et al, in "A hybrid approach for image security by combining encryption and steganography" 2013 [10],** the authors describe Multimedia data is more used on internet so it is desired to secure the data before transmitting. Various algorithms have been researched and proposed in this regards. This paper presents the hybrid approach for image security that combines both encryption and steganography. First the image is encrypted using proposed new version of AES algorithm, which is then hided into cover image using the steganography concept. Experimental results and analysis is shown. This hybrid approach provides greater security against attacks.

**ZuYing Wang et al, in "Experiments on Partial Encryption Performance for Image Sets" 2006 [11],** the authors describe This paper reports their experiments on the effectiveness of partial encryption for image sets. Professional image databases often contain a large number of similar images. This fact provides a unique opportunity for partial encryption coding. When the image set is stored as a representative image (the average) and the differences between the originals and the average, one could either encrypt a small percentage of every image in the set, or encrypt the average image partially and a tiny portion of each difference image. In their experiment, the portion to be encrypted is simply hidden from the reconstruction algorithm. No actual encryption algorithm is used. The performance of encrypting (hiding) different portions of the image set is evaluated by visual inspection and by the PSNRs between the original and the reconstructed images. Our algorithm is presented in detail and a Webcam image set and an ultrasound image set are used in the test. Hiding the average and portions of the differences provides a better encryption performance with a small fraction of the computation cost, compared to partial encryption of all original images

## VII. CONCLUSION AND FUTURE SCOPE

Disadvantage of employing RSA established RSA picture Encryption cryptography for encryption is speed. There are countless secret-key encryption methods that are considerably faster than each presently obtainable RSA picture Encryption method. Nevertheless, RSA picture cryptography can be utilized alongside secret-key cryptography to become the best of both worlds. For encryption, the best resolution is to join public- and secret-key arrangements in order to become both the protection gains of RSA picture arrangements and the speed gains of secret-key systems. RSA picture cryptography could be vulnerable to impersonation, even if users' confidential keys are not available. A prosperous attack on a certification power will permit an antagonist to impersonate whomever he or she chooses by employing a RSA picture certificate from the compromised power to attach a key of the adversary's choice to the term of one more user. RSA picture cryptography is not vital and secret-key cryptography alone is sufficient. These contain settings whereas safeguard hidden key allocation can seize locale, for example, by users encounter in private. It additionally includes settings whereas a solitary power knows and manages all the keys, for example, a closed investment system. As the power knows everyone's keys by now, there is not far supremacy for a little to be "public" and others to be "private." Note, though, that such a arrangement could come to be impractical if the number of users becomes large; there are not vitally each such limitations in a RSA picture system. In upcoming we will work on an Effectual Picture Encryption Strategy alongside Low intricacy employing Block Encryption.

## VIII. REFERENCES

[1]. Bagheri, M.; Taheri, M.; Mohammadi, K.; Mosavi, M.R.,"Evolution of mapping functions for image encryption using Evolvable Hardware",IEEE,Telecommunications (IST), 2010 5th International Symposium on,2010

[2]. Metzler, R.E.L.; Agaian, S.S.,"Selective region encryption using a fast shape adaptive transform",IEEE,Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on,2010

[3]. Seyedzadeh, S.M.; Moosavi, S.M.S.; Mirzakuchaki, S.,"Using self-adaptive coupled piecewise nonlinear chaotic map for color image encryption scheme",IEEE,Electrical Engineering (ICEE), 2011 19th Iranian Conference on,2011

[4]. Dan-hua Liu; Guang-ming Shi; Da-hua Gao; Min Gao,"A robust image encryption scheme over wireless channels",IEEE,Wireless Communications & Signal Processing, 2009. WCSP 2009. International Conference on,2009

[5]. Nini, B.,"Projection based permutation of color images",IEEE,Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on,2012

[6]. Sajasi, S.; Eftekhari-Moghadam, A.-M.,"A high quality image hiding scheme based upon noise visibility function and an optimal chaotic based encryption method",IEEE,AI & Robotics and 5th RoboCup Iran Open International Symposium (RIOS), 2013 3rd Joint Conference of,2013

[7]. Shang-Lin Hsieh; Hsuan-Chieh Huang; I-Ju Tsai,"A Copyright Protection Scheme for Gray-Level Images Using Human Fingerprint",IEEE,Information Technology: New Generations, 2006. ITNG 2006. Third International Conference on,2006

[8]. Junling Ren,"Information hiding algorithm for palette images based on HVS",IEEE,Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on,2010

[9]. Lukac, R.; Plataniotis, K.N.,"Digital image indexing using secret sharing schemes: a unified framework for single-sensor consumer electronics",IEEE,Consumer Electronics, IEEE Transactions on,2005

[10]. Saini, J.K.; Verma, H.K.,"A hybrid approach for image security by combining encryption and steganography",IEEE,Image Information Processing (ICIIP), 2013 IEEE Second International Conference on,2013

[11]. ZuYing Wang; Ping Luo; Xiaobo Li,"Experiments on Partial Encryption Performance for Image Sets",IEEE,Signal Processing and Information Technology, 2006 IEEE International Symposium on,2006