# A Study on Different Techniques for Security of an Image

Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V

***Abstract*: With the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important. Over the last few years several encryption algorithms have applied to secure image transmission. This paper is a review on the aspects and approaches of design an image cryptosystem. First a general introduction given for cryptography and images encryption and followed by different techniques in image encryption and related works for each technique surveyed. Finally, general security analysis methods for encrypted images are mentioned.***

***Index Terms*: Analysis, Cryptography, Encryption, Image, Image Transmission, Security.***

## I. INTRODUCTION

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is data Decryption, which recuperate the original data. Since cryptography first known usage in ancient Egypt it has passed through different stages and was affected by any major event that affected the way people handled information. In the World War II for instance cryptography played an important role and was a key element that gave the allied forces the upper hand, and enables them to win the war sooner, when they were able to dissolve the Enigma cipher machine which the Germans used to encrypt their military secret communications [1]. In modern days cryptography is no longer limited to secure sensitive military information but recognized as one of the major components of the security policy of any organization and considered industry standard for providing information security, trust, controlling access to resources, and electronic financial transactions. The original data that to be transmitted or stored is called plaintext, the one that can be readable and understandable either by a person or by a computer. Whereas the disguised data so-called ciphertext, which is unreadable, neither human nor machine can properly process it until it is decrypted. A system or product that provides encryption and decryption is called cryptosystem. Cryptosystem uses an encryption algorithms which determines how simple or complex the encryption process will be, the necessary software component, and the key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the data [2] [3]. In the 19th century, a famous theory about the security principle of any encryption system has been proposed by Kerchhoff. This theory has become the most important principle in designing a cryptosystem for researchers and engineers. Kirchhoff observed that the encryption algorithms are supposed to be known to the opponents. Thus, the security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm itself. For even though in the very beginning the opponent doesn't know the algorithm, the encryption system will not be able to protect the ciphertext once the algorithm is broken. The security level of an encryption algorithm is measured by the size of its key space [3]. The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the higher the security level is. In encryption, the key is piece of information (value of comprise a large sequence of random bits) which specifies the particular transformation of plaintext to ciphertext, or vice versa during decryption. Encryption key based on the keyspace, which is the range of the values that can be used to assemble a key. The larger keyspace the more possible keys can be constructed (e.g. today we commonly use key sizes of 128,192,or 256 bit , so the key size of 256 would provide a 2256 keyspace) [3][4]. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together. Depend on the algorithm, and length of the key, the strength of encryption can be considered. Assume that if the key can be broken in three hours using Pentium 4 processor the cipher consider is not strong at all, but if the key can broken with thousand of multiprocessing systems within a million years, then the cipher is pretty darn strong. There are two encryption/decryption key types: In some of encryption technologies when two end points need to communicate with one another via encryption, they must use the same algorithm, and in the most of the time the same key, and in other encryption technologies, they must use different but related keys for encryption and decryption purposes. Cryptography algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys).

**Revised Manuscript Received on 30 January 2013.**

* Correspondence Author

**Parameshachai B D***, Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Vacoas, Mauritius. (Research Scholar, Jain University, Bangalore).

**Dr. K. M. Sunjiv Soyjaudah**, Professor, Department of Electrical & Electronic Engineering, University of Mauritius, Reduit, Mauritius.

**Dr.Chaitanyakumar M V**, Principal & Professor Department of Electronics and Communication Engineering, Bearys Institute of Technology, Mangalore, India.

### A. *Symmetric key Algorithms*

In symmetric key encryption, the sender and receiver use the same key for encryption and decryption. As shown in figure 1. symmetric key encryption is also called secret key, because both sender and receiver have to keep the key secret and properly protected[4][5] Basically, the security level of the symmetric keys encryption method is totally depend on how well the users keep the keys protected. If the key is known by an intruder, then all data encrypted with that key can be decrypted.

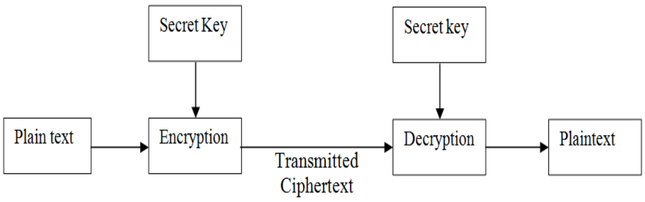


**Figure 1. Symmetric key Algorithms**

This is what makes it more complicated how symmetric keys are practically shared and updated when necessary. Symmetric keys can provide confidentiality but they can not provide authentication, because there is no way to prove through cryptography who actually sent a massage if two people are using the same key. Due to that, with all the problem and defects that symmetric keys have they still used in many applications, because they are so fast and can be hard to break if using a large key size. Symmetric keys can handle a large amount of data that would take an unacceptable amount of time with asymmetric keys to encrypt and decrypt.

The most popular symmetric key algorithms are Data Encryption Standard (DES), Triple DES, and Advance Encryption.

#### *i) The Data Encryption Standard (DES)*

DES is one of the most important examples of a block cipher. DES was the result of a contest set by the U.S. National Bureau of Standards (now called the NIST) in 1973, and adopted as standard applications in 1977. The winning standard was developed at IBM, as a modification of the previous system called LUCIFER. The DES is widely used for encryption of PIN numbers, bank transactions, and the like. The DES is an example of a block cipher, which operates on blocks of 64 bits at a time, with an input key of 64 bits. Every 8th bit in the input key is a parity check bit which means that in fact the key size is effectively reduced to 56 bits[6][7].

#### *ii) Advance Encryption Standard (AES)*

In 1997, the NIST called for submissions for a new standard to replace the aging DES. The contest terminated in November 2001with the selection of the Rijndael cryptosystem as the Advanced Encryption Standard (AES) [4] [8]. The Rijndael cryptosystem operates on 128-bit blocks, arranged as 4 × 4 matrices with 8-bit entries. The algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits.

### B. *Asymmetric key Algorithms*

Asymmetric key algorithm is also called public key algorithm. Public Key Cryptography was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976[9]. They described a two-key crypto system in which two parties could securely communicate over a non-secure communications channel without having to share a secret key and address the problem of secret key distribution by using two keys instead of a single key . In public key algorithm there are two keys are used. A public key, which can be known by everyone, and a privet key, which should be kept secret known only by the owner. As shown in figure 2.

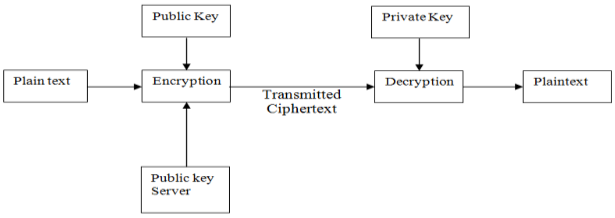


**Figure 2. Asymmetric key Algorithms**

If the massage is encrypted by one key the other key is required in order to decrypt the message [4]. The public key and private key are mathematically related. However it does not mean that, if someone got the public key he/she will be able to figure out the private key , but if someone got the private key, then here is big trouble, because private key should be accessed only by the owner no one else [4][5].

On the condition that the authentication is required, the data would be encrypted with the sender's private key then each person has the corresponding public key will be able to decrypt the data. This provides a confidence to the receiver that the data has been encrypted by one who has the possession of that private key. Encrypting data with private key is called *open message format*, since confidentiality is not ensured. Anyone with a copy of the corresponding public key can decrypt the data. The most popular asymmetric key algorithms are Rivest- Shamir Adelman (RSA).

#### *i) Rivest- Shamir Adelman (RSA)*

RSA is one of the most used public key algorithms today. This algorithm was invented in 1977 by Ron Rivest, Adi Shamir, and Len Adelman. The RSA is based on the idea of factorization of integers into their prime. Assume that Alice and Bob want to communicate with one other. Bob chooses two distinct large primes p and q and multiplies them together to form N, N = p*q. He also chooses an encryption exponent e, such that the, greatest common divisor of e and [(p-1)*(q-1)] is 1. That is gcd(e,[(p-1)*(q-1)])=1. He computes his decryption key d, d=1/e (mod [( p-1)*(q-1)]). Now he makes the pair (N,e) public and keeps p and q secret. This how to Generating keys, Encryption and decryption are of the following form, for some plain text block M and ciphertext block C: C=Me mod n, M= Cdmod n = (Me) mod n = Medmod n Both sender and receiver must know the values of n and e, and only the receiver knows the value of d. this make a public key encryption of KU = {e,n} and private of KR {d,n}.

## II. SYMMETRIC KEY ALGORITHMS VS. ASYMMETRIC KEY ALGORITHMS

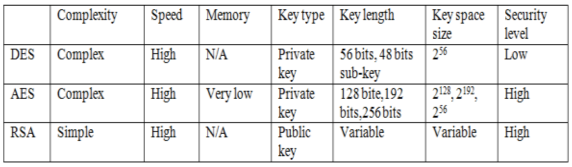
Asymmetric algorithms work much slowly then the symmetric algorithm, because they use more complex mathematics to perform their functions, which require more processing time.

With public key, you can just send out your public key to all of the people whom you need to communicate with, instead of keeping track of a unique for each one of them. The following list of the advantage and disadvantage of symmetric and Asymmetric key systems shown below.

- Symmetric key is much faster than asymmetric systems. On the other side asymmetric key Works much more slowly.
- In symmetric key the security is dependent on the length of the key, if using a large key size the algorithm will be hard to break, because symmetric algorithms carry out relatively simplistic mathematical functions on the bits during the encryption and decryption processes.
- Symmetric key requires a secure mechanism to deliver keys properly. While, asymmetric key provide a better key distribution than symmetric systems.
- Symmetric key provides confidentiality but not authenticity, because the secret key is shard. However, asymmetric key can provide authentication and confidentiality.

In symmetric key Each pair of users needs a unique key, if a user has N trading partners, then N secret keys must be maintained so as the number of individuals increases, so does the number of keys. However, management of the symmetric keys becomes problematic. Table 1 shows the comparative results of the encryption algorithms.

**Table 1. Compartaive Results of the Encryption Algorithms**



| | Complexity | Speed | Memory | Key type | Key length | Key space size | Security level |
|---|---|---|---|---|---|---|---|
| DES | Complex | High | N/A | Private key | 56 bits, 48 bits sub-key | $2^{56}$ | Low |
| AES | Complex | High | Very low | Private key | 128 bite,192 bits,256 bits | $2^{128}$, $2^{192}$, $2^{56}$ | High |
| RSA | Simple | High | N/A | Public key | Variable | Variable | High |

## III. IMAGE ENCRYPTION TECHNIQUES

### *A. Image Encryption*

The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image data have special properties such as bulk capacity, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique.

### *B. Public Key Image Encryption*

In some applications we dont have a secure channel to transmit the private key or prefer to keep the decryption key secretly, so we have to use public key cryptography. First public key algorithm published by Diffie and Hellman in 1976 [10]. It was a key exchange practical method for establishing a shared secret key over an authenticated communication channel without using a prior shared secret. Most of traditional public key cryptosystems designed to encrypt textual data. Some works have been published on public key image encryption, one is proposed by Shuihua et al. [11]. In this scheme, the plain image divided into blocks using a certain matrix transformation and all pixels in each block transferred to DCT domain. Public key, private key, encryption process and decryption process are defined based on transformation matrix of DCT coefficients. The results demonstrate that this technique is robust against JPEG lossy compression and other general attacks. Another public key technique based on Chebyshev chaos map described by K. Ganesan et al. [12] to encrypt color images and videos in real time applications. First they tried to cryptanalysis the encryption based on Chebyshev polynomial map and results show that it is not robust on some attacks, so they tried to enhance the security by using a non-XORing hash function to secure it against chosen plaintext attack. They do efficiency check and some testing for cryptanalysis such as key sensitivity, correlation, mono bit, long run test and time analysis for both image and video and concluded from the results that their proposed cryptosystem is more secure and robust to any intruder attack and the time analysis demonstrates the efficiency of encryption for 64x64 and 128x128 video encryption. An image encryption method using ECC is proposed by K. Gupta et al. [13] by transforming every pixel into the elliptic curve point to convert the plain image to encrypted image. They only proposed a framework and experiments done with a simple elliptic curve function with few points, so it is not an applicable system, but as a new idea, results show the acceptable encryption time in comparison with other public key techniques like RSA due to key size, and also provides the key sensitivity but needs to be enhanced as future works. Visual cryptography (VC) is a very easy and safe method suggested by Naor and Shamir [14] in 1994. In [15] A. Jaafar and A. Samsudin proposed a new public key scheme with simple and low computation by combination of VC and Boolean AND operation results a fast running time for encryption and decryption.

### C. Partial Encryption

Partial encryption also known as selective encryption, soft encryption or perceptual encryption is an approach that proposed to avoid encrypting the entire of an image. The main motivation is to reduce the computation time for real-time applications that runtime performance is often critical without compromising the security of the transmission too much. The main goal is to separate the image content into two parts, public part and protected part. One important feature in partial encryption is to make the protected part as small as possible. Partial encryption usually comes with compression. In frequency domain, low frequency coefficients carry the most information of the image and high frequency coefficients carry the details [16]. In lossy compression techniques such as JPEG standard, an image transforms to a frequency domain by DCT and then some high frequency coefficients are multiplied by zeros and new compressed image is reconstructed. So we can encrypt only some low frequency coefficients rather than all in frequency domain that also has many advantages [17]: i. It is easier to identify the critical parts to be encrypted and ii. It is easier to identify what parts of the data are not compressible. One of the first studies on selective multimedia encryption was done by Maples et al. in 1995 [18] by proposing Aegis mechanism based on MPEG video transmission and DES cryptosystem to secure MPEG video sequences from unauthorized access. This mechanism limits the amount of data to be encrypted or decrypted by using video compression to reduce the size of transmitted video images by encrypting intra I frames of an MPEG stream but .

Agi and Gong [19] found that this and some other methods are not adequate for sensitive applications and may not be sufficiently secure for some types of video and one can see pattern of movements, so they tried to improve the security by increasing the I-frame frequency but it causes to increase of bandwidth consumption and higher computational complexity. An alternative way is to encrypting I-blocks in all frames rather that I-frames that improves security. Droogenbroeck also proposed two techniques for selective encryption of both compressed and uncompressed images [20]. A selective encryption approach for uncompressed image is to encrypt 4 to 5 least significant bits because it is random like and plaintext attack on random like data is harder. Another selective encryption method that mentioned in this paper is based on compressed JPEG images and encrypts a selected number of AC coefficients. Results on execution time on three different encryption algorithms (DES, 3-DES and IDEA) show that real-time processing is easily achievable. Another technique for real-time applications by Droogenbroeck [21] that encrypts appended bits corresponding to a selected number of AC coefficients for each DCT block and he concluded that this scheme provides flexibility, multiplicity, spatial selectivity and format compliance. A multilevel partial image encryptionv(MPIE) proposed in [22] that performs the encryption before compression. Encryption is performed on parts of low frequency coefficients that determined by Haar Wavelet, and DFT applied on the approximation coefficients and a permutation matrix as encryption key is used to permute the result of transformation and then compression is doing by Huffman coding. Regardless of limitations such as complexity, low rate of compression and time consuming of this algorithm, some advantages are security, flexibility to image transformations and compression techniques. Another different approach in partial image encryption is to extract some special and secret features in an image and encrypt these features rather than encrypting the whole image. An idea in this scope is to detect faces of input image and encrypt them, for some applications such as transmission of images with guilty, accused persons or members of security organizations or military applications. K. Hong and K. Jung [23] proposed a partial encryption method using the face region as a feature because a face has the semantic information and is the most important part in an image or video. They used Multi-Layer Perceptrons to detect face region and for more exact, Gaussian skin-color applied to discriminate between skin regions and non-skin regions. Both DES and AES encryption algorithms are compared and results shows that encryption time is less for DES. Due to experiments, for video content encryption, fully encryption methods provide 2 or 3 frames in a second but their proposed method encrypts 25 to 30 frames per seconds. A different scheme by J. M. Rodrigues et al. [24] for selective encryption in video offered also for face protection based on AES stream cipher for JPEG image sequences by performing three steps on DCT blocks. These steps are respectively construction of plain text, ciphering the plain text and substitution of the original Huffmans vector with the ciphered information. This scheme provides advantages such as portability, constant bit rate and selective encryption of the region of interest and doesnt effects on all the JPEG compression rate, which makes it useful for a large range of applications with good information confidentiality results. JPEG2000 is a widely used compression standard based on wavelet transform. S. Lian et al. [25] proposed a selective image encryption scheme based on JPEG2000. They reduced the encryption data ratio to less than 20% by selecting significant bit-planes of wavelet coefficients in high and low frequency, so the encryption time ratio deducted to less than 12%. Their experiments show the security of their scheme against brute-force attack, select plaintext attack or replacement attack and does not effects on compression ratio. Another recent selective encryption based on wavelet transform in fractional wavelet domain published by N. Taneja et al. [26]. In this work, 3.125% of significant image data selected by normalized information energy (NIE) and encrypted these selected subbands by Arnold cat map, a 2D chaotic function.

### *D. Digital Signature for Image Authentication*

The act of digital signature is similar to handwritten on paper signature which playing the main role in authenticating documents and verify the identity. Hence, digital signature has many applications in information security. It is a mechanism that providing authentication, data integrity and non-repudiation. The firs concept of digital signature was a scheme based on RSA [27] in many years ago and today is one of the most practical techniques. Most of the digital signatures are based on asymmetric cryptography. In these systems, the private key is used to create a digital signature that uniquely proofs the signer who is holder of the private key and can be authenticated only with the corresponding public key. One of the first researches on digital signature and its applications in images refers to an article published in 1998 by C. Yung Lin and S. Chang [28]. They proposed a robust digital signature based on DCT coefficients in JPEG images. This generated digital signature is robust to cropping, intensity changes, resizing and applying filters. Digital signature and watermarking are related and both used for authentication but there is slightly differences in their structure. Tao Chen et al. tried to combine digital signature with watermarking [29]. The advantage of this combination is to save the required bandwidth for signature which is encoded to a separate file. To achieve this aim, they embed the signature file as a watermark, so their proposed scheme not only capable to authenticate the image, but also can perform a copyright protection. Another image authentication scheme [30] use the content of an image wavelet transform domain to construct a structural digital signature. They showed that this scheme is robust to content-preserving manipulations and fragile to content-changing distortions. A scheme based on a combination of generalized synchronization Henon discrete-time chaotic system which uses as a pseudo-random number generator to establish encryption and digital signature is proposed by H. Zang et al. [31]. The large key space as 10158, sensitivity to confusion of parameters and initial condition because of applying chaos in encryption make this scheme confident to be used in secure communication.

### *E. Chaotic Encryption*

Chaos-based encryption is one of the applications of the nonlinear dynamics of chaotic finder. It meets the issues that are creating the problem of encryption, the different kinds of image encryption techniques that are based on the chaotic schemes are discussed in the following paragraphs.

Qiang Wang et al have undergone a research on the digital image encryption which is based on the DWT (discrete wavelet transform) and Chaos. In this discussion, a digital image watermark algorithm has been developed that is based on the concept of discrete wavelet transform (DWT) and chaos theory. First, the discrete wavelet transform has to be done to retrieve the low frequency part as embedding field; secondly the chaotic sequence has to be done to encrypt the watermark to retrieve the low frequency, and to embed with the original image. As the result of this, this technique promote the resistance on JPEG compression, noise attack, filter and so on [32].

Yong-Hong Zhanghas designed and developed an image encryption using extended chaotic sequences. In this study, the chaotic cryptography technique is used which is called a key cryptography. Here, the extended chaotic processes are generated by using the *n* -rank rational Bezier curve. Results shows that the high key space and good security level [33]. Monisha Sharma and Manoj Kumar Kowar have done a review on image encryption techniques using chaotic schemes. In this manuscript, the chaotic image encryption is made possible by the parameters of chaos which includes the deterministic dynamics, unpredictable behavior and non-linear transform. Which leads to the techniques that provide security features and a complete visual check [34]. Mintu Philip and Asha Das have jointly done a survey on image encryption process by using the chaotic cryptography schemes. The author states that the cryptography uses the chaotic system features namely the loss of information and the initial condition from sensitive condition. They have concluded the paper with comparisons made out of the performance of the existing chaotic image encryption methods [35]. Jun Lang, Ran Tao, Yue Wang has proposed an image encryption technique which is based on the concept of multiple parameter discrete fractional Fourier transform and the chaos function. In this paper, the image is encrypted by the position of the images in many arguments of the discrete fractional Fourier block whereas the alignment of the sections is evaluated by chaotic logistic maps. As the result of this, comparison has been made in between the various existing schemes and posses' good or superior robustness [36].

## IV. SECURITY ANALYSIS OF THE ENCRYPTED IMAGE

Use Security analysis is the art of find the weakness of a cryptosystem and retrieval whole or a part of a ciphered message (in this area, an image) or finding the secret key without knowing the decryption key or the algorithm. There are many techniques for applying analysis, depending on what access the analyst has to the plaintext, ciphertext, or other aspects of the cryptosystem. Below are some of the most common types of attacks to encrypted images:

### *A. Key Space Analysis*

Try to find the decryption key by checking all possible keys. The number of try to find directly refers to key space of the cryptosystem grow exponentially with increasing key size. It means that doubling the key size for an algorithm does not simply double the required number of operations, but rather squares them. An encryption algorithm with a 128 bit in key size defines a key space of 2128, which takes about 1021 years to check all the possible keys, with high performance computers of nowadays. So a cryptosystem with key size of 128 bit computationally looks robust against a brute force attack.

### *B. Statistical Analysis*

Statistical attack is a commonly used method in cryptanalysis and hence an effective cryptosystem should be robust against any statistical attack. Calculating the histogram and the correlation between the neighbors pixels in the source and in the encrypted image are the statistical analysis to prove the strong of the proposed cryptosystem against any statistical attack. Statistical analyzing demonstrates the relation between the original and encrypted image. Therefore, encrypted image must be completely different from the original. Due to Shannon theory [17] It is possible to solve many kinds of ciphers by statistical analysis. For an image there are some ways to determine whether the ciphered image leaks any information about the original one or not.

### *C. Correlation Analysis*

Two adjacent pixels in a plain image are strongly correlated vertically and horizontally. This is the property of an image, the maximum value of correlation coefficient is 1 and the minimum is 0, a robust encrypted image to statistical attack should have a correlation coefficient value of 0.

### *D. Differential Analysis*

The aim of this experiment is to determine the sensitivity of encryption algorithm to slight changes. If an opponent can create a small change (e.g. one pixel) in the plain image to observe the results, this manipulation should cause a significant change in the encrypted image and the opponent should not be able to find a meaningful relationship between the original and encrypted image with respect to diffusion and confusion, the differential attack loses its efficiency and become useless.

### *E. Key Sensitivity Analysis*

In addition of large enough key space to resist a cryptosystem at brute force attack, also a secure algorithm should be completely sensitive to secret key which means that the encrypted image cannot be decrypted by slightly changes in secret key.

## V. CONCLUSION

Security of digital images in transmission, publishing and storage become more important due to ease of access to open networks and internet. In this paper a surveyed of the currently known methods of cryptography were presented. The two different types of the encryption methods (Symmetric key encryption and Asymmetric key encryption) were highlighted and evaluated with respect to their security level and encryption speed. A discussed about the advantages and disadvantages of each of them. Also we have surveyed existing research on image encryption in a new approach by classification different types of work using other techniques more than only encryption. These techniques were partial encryption, chaos maps, public key and digital signature which applied to improve and enhance the efficiency of an image encryption algorithm.

*Published By:*
*Blue Eyes Intelligence Engineering*
*and Sciences Publication (BEIESP)*

Finally, general security analyzing techniques for encrypted images are given which use to evaluate the robustness of a cryptosystem.

Figure 3 shows briefly a classified representation of existing image encryption techniques and algorithms.

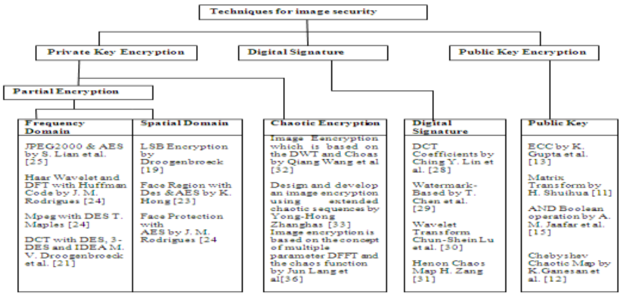

Techniques for image security
Private Key Encryption
Digital Signature
Public Key Encryption
Partial Encryption
Frequency Domain
Spatial Domain
Chaotic Encryption
Digital Signature
Public Key
JPEG2000 & AES by S. Lian et al. [25]
Haar Wavelet and DFT with Huffman Code by J. M. Rodrigues [24]
Mpeg with DES T. Maples [24]
DCT with DES, 3-DES and IDEA M. V. Droogenbroeck et al. [21]
LSB Encryption by Droogenbroeck [19]
Face Region with Des &AES by K. Hong [23]
Face Protection with AES by J. M. Rodrigues [24
Image Eencryption which is based on the DWT and Choas by Qiang Wang et al [32]
Design and develop an image encryption using extended chaotic sequences by Yong-Hong Zhanghas [33]
Image encryption is based on the concept of multiple parameter DFFT and the chaos function by Jun Lang et al[36]
DCT Coefficients by Ching Y. Lin et al. [28]
Watermark-Based by T. Chen et al. [29]
Wavelet Transform Chun-Shein Lu et al. [30]
Henon Chaos Map H. Zang [31]
ECC by K. Gupta et al. [13]
Matrix Transform by H. Shuihua [11]
AND Boolean operation by A. M. Jaafar et al. [15]
Chebyshev Chaotic Map by K.Ganesan et al. [12]

**Figure 3. Classified hierarchical diagram of existing image encryption techniques.**

## REFERENCES

1. Kahn, David , (1980). Cryptology Goes Public, Communications Magazine, IEEE.
2. Kessler , Gary C., (1998). An Overview of Cryptography.
3. B. White, Gregory, (2003). Cisco Security+ Certification: Exam Guide, McGraw-Hill.
4. Shon harris, (2007). SICCP Exam Guide, fourth edition, McGraw-Hall
5. Stallings, William, (2007). Network Security Essentials, applications and Standards , Pearson Education, Inch.
6. Wayne G. Barker, "Introduction to the analysis of the Data Encryption Standard (DES)", A cryptograph-ic series, Vol. 55, p. viii + 190, Aegean Park Press, 1991.
7. Kofahi, N.A., Turki Al-Somani, Khalid Al-Zamil. “Performance evaluation of three encryption/decryption algorithms” 2005 IEEE International Symposium on Micro-NanoMechatronics and Human Science, Publication Date: 30-30 Dec. 2003. Volume: 2, pp 790-793.
8. Jean-Yves chouinard.,. Design of secure computer systems CSI4138/CEG4394 notes on the advanced encryprion standard (AES).
9. Diffie , Whitfield & Hellman, Martin E, (1976) . New Directions In Cryptography, IEEE TRANSACTIONS ON INFORMATION THEORY.
10. W. Diffie and M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, Issue 6, Nov 1976.
11. H. Shuihua and Y. Shuangyuan, An Asymmetric Image Encryption Based on Matrix Transformation, Transactions on Computer and Information Technology, Vol. 1, No. 2, 2005.
12. K.Ganesan, I. Singh and M. Narain, Public Key Encryption of Images and Videos in Real Time Using Chebyshev Maps, Fifth International Conference on Computer Graphics, Imaging and Visualization, 2008.
13. K. Gupta, S. Silakari, R. Gupta and S. A. Khan, An Ethical way for Image Encryption using ECC, First I. Conference on Computational Intelligence, Communication Systems and Networks, 2009.
14. M. Naor and A. Shamir, Visual cryptography, Advances in Cryptology- EUROCRYPT94, Lecture Notes in Computer Science, Vol. 950, Springer-Verlag, Berlin, pp. 1-12, 1995.
15. A. M. Jaafar and A. Samsudin, A New Public-Key Encryption Scheme Based on Non-Expansion Visual Cryptography and Boolean Operation, Int. Journal of Computer Science Issues, Vol. 7, Issue 4, No. 2, July 2010.
16. W. Effelsberg and R. Steinmetz, Video Compression Techniques, Heidelberg, Germany: Dpunkt-Verlag, 1998.
17. W. Zeng and S. Lei, Efficient Frequency Domain Selective Scrambling of Digital Video, IEEE Transactions on Multimedia, 5(1), March 2003
18. T. Maples and G. Spanos, Performance study of a selective encryption scheme for the security of networked real-time video, Proceedings of the 4th International Conference on Computer Communications and Networks, Las Vegas, 1995.
19. I. Agi and L. Gong, An empirical study of secure MPEG video transmission, Symposium on Network and Distributed Systems Security, 1996.
20. M. V. Droogenbroeck and R. Benedett, Techniques for a selective encryption of uncompressed and compressed images, Proceedings of ACIVS, Ghent, Belgium, September 2002.
21. M. V. Droogenbroeck, Partial Encryption of Images for Real-Time Applications, 4th IEEE Signal Processing Symposium, Hilvarenbeek, The Netherlands, pp. 11-15, 2004.
22. O. M. Odibat, M. H. Abdallah and M. B. Al-Zoubi, New Techniques in the Implementation of the Partial Image Encryption , 4th International Multi-conference on Computer Science and Information Technology, Jordan, 2006.
23. K. Hong and K. Jung, Partial Encryption of Digital Contents Using Face Detection Algorithm, Springer-Verlag, 2006.
24. J. M. Rodrigues, W. Puech, P. Meuel, J. C. Bajard and M. Chaumont, Face Protection by Fast Selective Encryption in a Video, The Institution of Engineering and Technology Press, Seattle, WA, 1993.
25. S. Lian, J. Sun, D. Zhang and Z. Wang, A Selective Image Encryption Scheme Based on JPEG2000 Codec, LNCS 3332, pp. 6572, Springer-Verlag, Berlin Heidelberg, 2004.
26. N. Tanejaa, B. Ramanb, I. Guptaa, Selective image encryption in fractional wavelet domain, In. Journal of Electronics and Communications, (AE) 65, pp. 338344, Elsevier, 2011.
27. Rivest, Shamir and Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21 (2): pp. 120126, 1978.
28. C. Y. Lin and S. Fu Chang, Generating Robust Digital Signature for Image/Video Authentication, Multimedia and Security Workshop at ACM Multimedia, Bristol, UK. , 1998.
29. T. Chen, J. Wang and Y. Zhou, Combined Digital Signature and Digital Watermark Scheme for Image Authentication, Int. Conferences on Infotech and Info-net, Beijing, 2001.
30. Chun-Shein Lu and H. Y. Mark Liao, Structural Digital Signature for ImageAuthentication: An Incidental Distortion Resistant Scheme, IEEE Transactions on Multimedia,Vol.5,No.2, 2003.
31. H. Zang, L. Min, Li Cao, An Image Encryption and Digital Signature Scheme Based on Generalized Synchronization Theorem, International Conference on Computational Intelligence and Security, 2009.
32. Qiang Wang, Qun Ding , Zhong Zhang, Lina Ding, “Digital Image Encryption Research Based on DWT and Chaos” *IEEE Transactions* pp. 494-498,2008.
33. Yong-Hong Zhang, “Image encryption using extended chaotic sequences”, *IEEE Transactions International Conference on Intelligent Computation Technology and Automation* pp. 143-146,2011.
34. Monisha Sharma et. al. “Image Encryption Techniques Using Chaotic Schemes: A Review” *International Journal of Engineering Science and Technology,* Vol. 6,pp. 2359-2363, 2010.
35. Mintu Philip, Asha Das, “ Survey: Image Encryption using Chaotic Cryptography Schemes” *International Jounal of Computer Applications,*2011.
36. Jun Lang, Ran Tao, Yue Wang, “Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function” *Optics Communications*, Vol 283, pp. 2092-2096, 2010.
37. R. Matthews, On the derivation of a chaotic encryption algorithm. Cryptologia, pp. 2942, 1989.

## AUTHOR PROFILE

**Parameshachari B D** working as a Senior Lecturer in the Department of Electronics and Communication Engineering at JSS Academy of Technical Education, Mauritius. He is having total of around nine and half years experience in the teaching field (including seven years from KIT, Tiptur and two and half years from JSSATE, Mauritius). Parameshachari B D obtained his B.E in Electronics and Communication Engineering from Kalpatharu Institute of Technology, Tiptur and M. Tech in Digital communication Engineering from B M S college of Engineering, Bangalore. He is pursuing his PhD in Electronics and Communication Engineering at Jain University, Bangalore under the guidance of Dr. K M Sunjiv Soyjaudah, University of Mauritius, Reduit, Mauritius. His current research includes image processing and cryptography. He has published several Research papers in international Journals/conferences. He is a Member of ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.

**Professor K M Sunjiv Soyjaudah** received his B. Sc (Hons) degree in Physics from Queen Mary College, University of London in 1982, his M.Sc. Degree in Digital Electronics from King’s College, University of London in 1991, and his Ph. D. degree in Digital Communications from University of Mauritius in 1998.

He is presently Professor of Communications Engineering in the Department of Electrical and Electronic Engineering of the University of Mauritius. His current interest includes source and channel coding modulation, image processing, cryptography, voice and video through IP, as well as mobile communication. Dr. K M S Soyjaudah is a member of the IEEE, Director in the Multicarrier (Mauritius), Technical expert in the Energy Efficiency Management Office, Mauritius.

**Dr. Chaitanyakumar M V** obtained his B.E from University Visweswaraiah College of Engg., Bangalore in 1983; He received his masters and doctoral degree from University of Roorkee, Roorkee (IIT-R), India in 1991 and 1994 respectively. He is a receipent of First Khosla research award from University of Roorkee in 1993. Presently Dr.Chaitanyakumar M V is serving as the Principal & Professor Department of Electronics and Communication Engineering, Bearys Institute of Technology, Mangalore, India. He has over thirty years experience in the teaching field. His current interest includes Antennas, Image processing. Microwave and Radar Engineering,

*Published By:*
*Blue Eyes Intelligence Engineering*
*and Sciences Publication (BEIESP)*
*© Copyright: All rights reserved*