International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:6, No:6, 2012

A Survey on Principal Aspects of Secure Image Transmission

Ali Soleymani, Zulkarnain Md Ali, and Md Jan Nordin

Abstract—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.

Keywords—Image, cryptography, encryption, security, analysis.

I. Introduction

THE need for information security is become inevitable due to rapid development and applications of computer networks and internet technology. Information needs to be secure as they are valuable resources of any organization like other resources such as hardware, software, employee, financial resources and legal position. Security consists of some policies, rules, protocols and standards that help the organization to meet the objectives and missions. Organizations need security to protect their assets from illegal and unauthorized access, also people in their personal life need to keep confidential their private documents, family albums and films. Physical security and access control is a solution but it is not enough. Electronic data are easy to access, steal or copy via networks, so we need more secure methods to keep them safe. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (ciphertext) and then retransforming that message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security and engineering. The three most important objectives of cryptography include (1) confidentiality, (2) data integrity, and (3) authentication. Confidentiality refers to the protection of information from unauthorized access. An undesired communicating third party (called adversary) must not be able to access the communication material. Data integrity ensures that information has not been manipulated in an unauthorized way. Finally, Authentication is the equivalent of a signature and studied in two concepts: entity authentication and message authentication. Message authentication provides assurance of the identity of the sender of a message. This type of authentication also includes evidence of data integrity because if the data are modified during transmission, the sender cannot be the originator of the message. Entity authentication assures the receiver of a message of both the identity of the sender and his active participation [1]. Digital images are attractive data types with widespread range of use and many users are interesting to implement content protection methods on them to keep from preview, copyright or manipulation. In many applications like military image databases, confidential video conferencing, medical imaging system, cable TV, online personal photograph album, security in essential. Also wide application of images in industrial process turns it into a resource and asset, so it is important to protect the confidential image data from unauthorized access. Most of todays encryption algorithms are based on textual data, but images are different from text. An idea for image encryption is to consider a 2D image as a 1D data stream and encrypt this stream with any textual based cryptosystem [2]-[5], this simple idea called as nave approach. This approach is usually suitable for text, and sometimes for small bitrate audio, image and video files that are being sent over a fast dedicated channel [6]. These encryption algorithms may not satisfy for different image data types like JPEG, PNG and BMP and not given proper attention to the sensitivity of image types. Although we may use the traditional cryptosystems to encrypt images directly, but it is not a good idea for two reasons. One is that images are different from text and the image size is almost always much greater than that of text. Due to large data size and real time constrains, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image may contain small distortion and usually it is acceptable. So those algorithms that are good for textual data may not be suitable for multimedia data. But many researches had done on using textual encryption algorithms for images and tried to adapting the algorithm with image properties.

A. Soleymani is with the School of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, 43600, Selangor, Malaysia. e-mail: ali.soleymani@ftsm.ukm.my

Z. Md Ali and M. Jan Nordin are with the School of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, 43600, Selangor, Malaysia. e-mail: zma@ftsm.ukm.my, jan@ftsm.ukm.my

II. Image Encryption Techniques

A. Classic Image Encryption

Advanced Encryption Standard (AES) is a symmetric cryptosystem that proposed for text encryption by Rijmen and Daemen in 1999 [7] and also known as Rijndael algorithm, but some researchers applied this algorithm for image encryption also with some modifications in key generation and other specification. Zeghid et al. [8] proposed a modified AES based algorithm for image encryption by adding a key stream generator (A5/1, W7) to AES to ensure improving the encryption

performance. Another algorithm proposed by Subramanyan et al. [9] based on AES Key Expansion in which the encryption process is a bit wise XOR operation of a set of image pixels along with a 128 bit key which changes for every set of pixels. The keys to be used are generated independently at the sender and receiver side based on AES Key expansion process hence the initial key is alone shared rather than sharing the whole set of keys. DES, a popular block cipher algorithm that uses 64 bit key, is another textual cryptosystem that used for image encryption by Qian Gong-bin et al. In [10] a new image encryption scheme based on DES combined with a chaotic map (Chaotic map will be explained completely in next section) presented to improve the security and expand the key space. The results show that combination of textual cryptosystems with other techniques or making some changes, improve the security and anti-attack ability of those algorithms effectively.

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 [11]. 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. [12]. 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. [13] 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. [14] 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 [15] in 1994. In [16] 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. Compression and Encryption

Compression techniques help us to reduce the transmission bandwidth or storage space. These techniques can be implemented in both spatial and frequency domain. Also frequency domain techniques are more efficient and using common and popular transforms such as DCT, DFT and DWT. Data compression studies can be divided into two categories: lossy and lossless. Lossy techniques concede a certain loss for data in exchange with the high compression ratio. Generally lossy techniques decrease the quality of the object so they are applied for images, videos and audios because of human perception. On the other hand, some kinds of data could not accept any loss (e.g. Database records, executable files and word processing files and medical images), otherwise the data will be degraded, and here the lossless techniques play role. Conventional cryptosystems relates to the compressed multimedia. Multimedia compression and encryption are usually very incompatible and a trade-off relies between them. Encrypting the multimedia content before compression removes a lot of redundancy and this result in a very poor compression ratio. On the other hand, encrypting the data after compression destroys the codec format, which causes decoders to crash. Finally, for many applications, we would like to have very light encryption that preserves some perceptual information [17]. B. Mohammed et al. [18] in their proposed encryption-compression method first imposed a FMT technique to compress the given image and then AES-Based algorithm applied to encrypt the image. L. Vorwerk et al. [19] tried to combine encryption and wavelet compression. The approach of encryption is using a symmetric key for encrypting image and wavelet filter, but for secure exchange of key, a public key cryptosystem is proposed to encrypt the symmetric key. A new combination of encryption and compression for images proposed by I. Masanori et al. [20] based on Independent Component Analysis (ICA) and Discrete Cosine Transform (DCT). To achieve a fast and secure image transmission they used DCT and a low pass filter for image compression and by rotating and mixing the DCT blocks with a random image the source image is encrypted. At destination, the encrypted received image is decrypted by extracting the covered images from the mixtures by applying ICA and finally by using rotation keys and IDCT the original image is reconstructed. Another approach to integrate of compression and encryption is designed in the system of C. Wu and J. Kuo [21]. They discussed about advantages and disadvantages of selective encryption and proposed an encryption schemes that modifies the entropy of plain message to result the cipher message by applying Huffman coder and QM coder. Finally, concluded that this high security scheme can be applied to compression techniques such as MPEG and JPEG with acceptable computational speed.

D. Selective Encryption

Selective encryption also known as partial 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 selective encryption is to make the protected part as small as possible. Selective 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 [22]. 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 [23]: 1. It is easier to identify the critical parts to be encrypted and 2. 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 [24] 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 [25] 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 [26]. 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 [27] 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 encryption (MPIE) proposed in [28] 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 [29] 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. [30] 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. [31] 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. [32]. 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.

E. Chaos Theory and Cryptography

Chaos theory is the study of nonlinear dynamical systems that are exhibit extreme sensitivity to initial conditions and have random like behaviors, discovered by Edward Lorenz in 1963 [33], an effect which is popularly referred to as the butterfly effect that has a definition: Does the flap of a butterflys wings in Brazil set off a tornado in Texas? The flapping wings represent a small change in the initial condition of the system, which causes a chain of events leading to large-scale phenomena. Had the butterfly not flapped its wings,

the trajectory of the system might have been vastly different [34]. Generally it means that small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for chaotic systems, rendering long-term prediction impossible in general. This happens even though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems makes them unpredictable [34]. This behavior is known as deterministic chaos, or simply chaos. Random like behavior, non-predictable and sensitivity to initial value are three features that make it an acceptable choice to relate it with cryptography. The only difference is that encryption operations are defined on finite sets of integers while chaos maps are defined on real numbers. Chaotic behaviors are exhibits by chaotic maps. These maps are classified by continuous maps and discrete maps. Discrete maps usually take the form of iterated functions. Iterates are similar to rounds in cryptosystems, so discrete chaotic dynamic systems are used in cryptography. Each map has some parameters that equivalent with encryption key in cryptography. The similarities and differences between these two subjects are listed in Table I [35]. According to [36], there are two general ways to apply a chaos map in a cipher system: 1) using chaotic systems to generate pseudo-random key stream; 2) using the plaintext or the secret key(s) as the initial conditions and control parameters then apply some iterations on chaotic systems to obtain ciphertext. The first way corresponds to stream ciphers and the second to block ciphers.

TABLE I
SIMILARITIES AND DIFFERENCES BETWEEN CHAOS AND CRYPTOGRAPHY

Chaotic Systems	Cryptographic Algorithms
Phase space: Set of real numbers	Phase space: Finite set of integers
Iterations	Rounds
Parameters	Key
Sensitivity to initial conditions and parameters	Diffusion

Matthews proposed the first chaotic encryption algorithm in 1989 [17]. After that, researches on chaos-based encryption developed and one of these first studies was done by Baptista [37]. He used simple one-dimensional logistic map to encrypt each character of a text message as the integer number of iterations performed in the logistic equation. Ge Xin et al. tried to analyzed Baptistas cryptosystem [38] and concluded that it has 2 defects, first is that the encryption speed is very slow in comparison with conventional cryptosystems because of large number of iterations and on the other hand the proposed method is not robust to known-plaintext attack, but it was the origin of utilization chaos in cryptography. M. Sharma and M. Kowar in their article [39] classified image encryption based on chaotic scheme in two groups: Spatial Domain and Frequency Domain. In spatial domain, Fridrichs published research [40], [41] was one of the first on chaos-based image cryptography in 1997. J. Yen and J. Guo [42] presented an algorithm which according to a chaotic binary sequence, the encrypted image generated by the gray level of each pixel is XORed or XNORed bit by bit to one of the two predetermined keys. Works on chaotic image encryption has been developed by trying different chaotic maps to overcome the traditional cryptosystem disadvantages and this technique found adequate for image encryption due to speed and strong security. A chaotic image encryption using Lorenz map by Sobhy [43] was proposed with application in image encryption, creating secure databases and secure Email which implemented in FPGA for real time images. One dimensional chaotic equation is another map which used by F. Belkhouche and U. Qidwai [44]. It has been shown that the method can be used for binary image encryption with the possibility of using several keys such as the initial state, the external parameters and the number of iterations. Non-linear map used for iterating pixel values by Z. Han and W. Xiu Feng [45]. Cat map combined with neural network by D. Shaojiang [46] and Arnold map by M. R. Zhang et al. [47] are other discrete chaotic maps which used in image encryption. Yiwei et al. in their novel image encryption algorithm [48] combined two chaotic maps and proposed an alternate structure to achieve higher strength rather than using one chaotic map. Chaotic functions in this scheme are one-way coupled map lattice (OCML) used for substitution and general cat-map for permutation and diffusion. These maps are applied in every round of encryption alternately and this combination results a large key space and resist to statistical attacks as analysis shown. Three different chaotic maps used for image encryption by M. Ahmad and M. S. Alam [49]. Applying 2D cat map on 8*8 blocks of an image to perform shuffling pixels, generating control parameters of shuffling randomly by 2D coupled logistic map and finally encrypting the shuffled image by 1D Logistic map results a very low correlation and information entropy very close to 8. So in this scheme there is no information leakage from encrypted image. Another composition of chaotic maps [50] is based on two logistic maps with different initial parameters to extend the key size as 104 bit and make the encrypted image safe to different types of attacks. Finally a combination of three encryption algorithms called Triple-Key chaotic is introduced by G. Srividya and P. Nandakumar [51] in 2011. These three keys are an 80-bit session key, initial parameter key and control parameter key. To implement their own scheme, they combine two previous works [52], [53] were based on logistic chaotic map and chaotic neural network respectively then using these maps to perform position permutation and value transformation of image pixels to achieve high security as their histogram analysis, correlation analysis and key sensitivity analysis results demonstrate.

F. 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 [54] 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 [55]. 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 [56]. 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 [57] 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. [58]. 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.

III. Security Analysis of Encrypted Image

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 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.

IV. 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, 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 compression, selection, chaos maps, public key and digital signature which applied to improve and enhance the efficiency of an image encryption algorithm. Finally, general security analyzing techniques for encrypted images are given which use to evaluate the robustness of a cryptosystem. Fig. 1 is briefly a classified representation of existing image encryption techniques and algorithms.

Acknowledgment

This work was supported by The Ministry of Higher Education Malaysia under research grant of FRGS/1/2012/SG05/UKM/02/1.

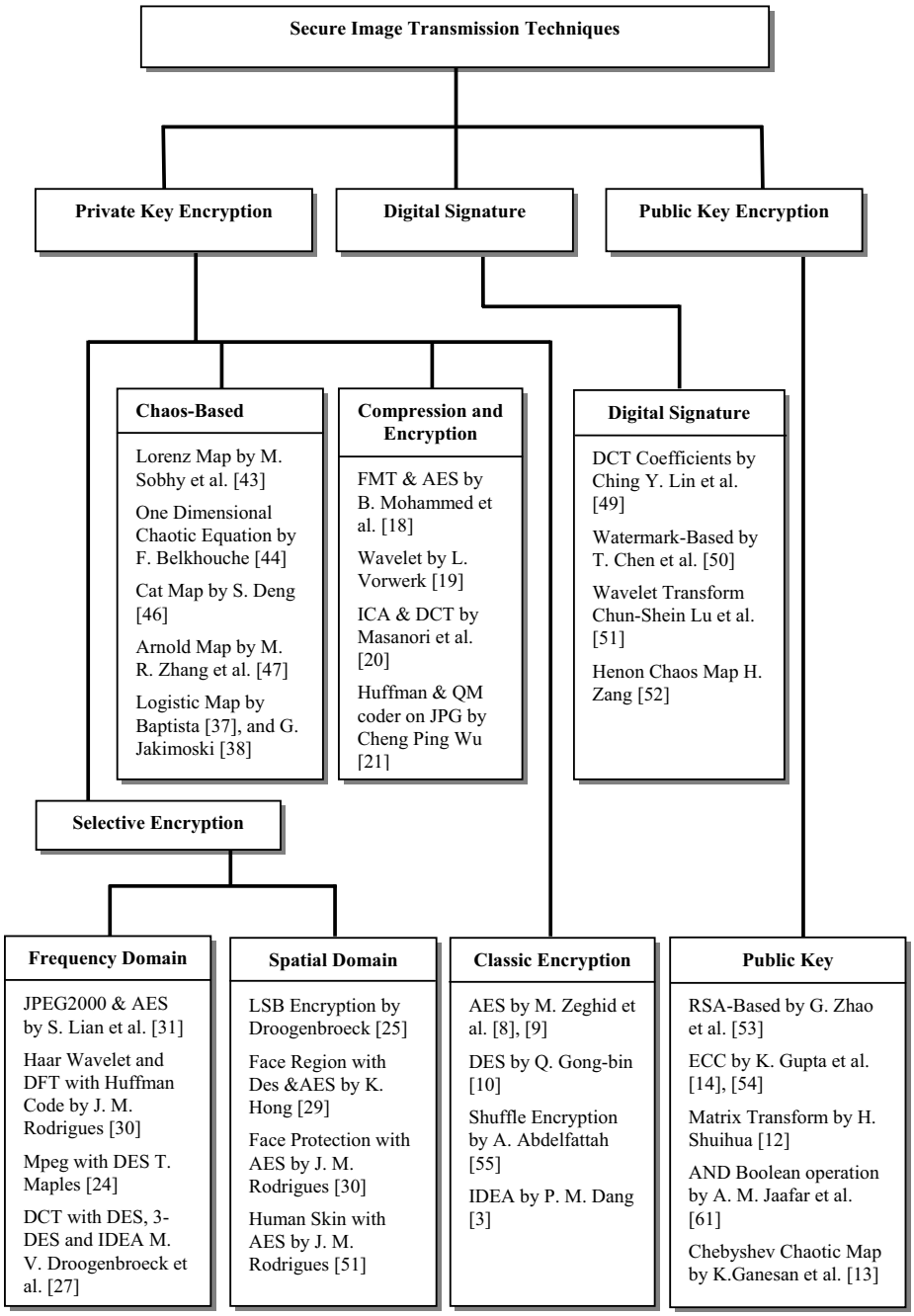

Fig 1. Classified hierarchical diagram of existing image encryption techniques.

REFERENCES

[1] B. Furht and D. Kirovski, Multimedia Security Handbook, CRC Press, USA, 2005.
[2] P. Dang and P. M. Chau, Image encryption for secure internet multimedia applications, IEEE Transaction on Consumer Eletronics, 46(3): pp. 395403, 2000.
[3] P. Dang and P. M. Chau, Implem1entation IDEA algorithm for image encryption, Mathematics and Applications of Data/Image Coding , Compression and Encryption, volume 4122 of Proceedings of SPIE, pp. 19, 2000.
[4] P. Dang and P. M. Chau, Hardware/software implementation 3-Way algorithm for image encryption, Security and Watermarking of Multimedia Contents II, volume 3971 of Proceedings of SPIE, pp. 274283, 2000.
[5] S. McCanne and V. Jacobson, A flexible framework for packet video, Proceedings of 3rd ACM International Conference on Multimedia, pp. 511522, 1995.
[6] B. Furht, E. Muharemagic and Daniel Socek, multimedia encryption and watermarking, Springer, 2005.
[7] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999.
[8] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, A Modified AES Based Algorithm for ImageEncryption, World Academy of Science, Engineering & Technology, 2007.
[9] B. Subramanyan, V. M. Chhabria, T. G. S. babu, Image Encryption Based On AES Key Expansion, Second International IEEE Conference on Emerging Applications of Information Technology, 2011.
[10] Q. Gong-bin, J. Qing-feng and Q. Shui-sheng, A New Image Encryption Scheme Based on DES Algorithm and Chuas Circuit, Int. Journal of Computer Science and Network Security, VOL.8, No.4, April 2008.
[11] W. Diffie and M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, Issue 6, Nov 1976.
[12] H. Shuihua and Y. Shuangyuan, An Asymmetric Image Encryption Based on Matrix Transformation, Transactions on Computer and Information Technology, Vol. 1, No. 2, 2005.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] R. Matthews, On the derivation of a chaotic encryption algorithm. Cryptologia, pp. 2942, 1989.
[18] B. Mohammed, G. Mourad, Z. Nourddine, R. Fakhita and B. ElHoussine, Encryption-Compression Method of Images, Int. Journal on Computer Science and Information Systems Vol. 4, No. 1, pp. 30-41, 2009.
[19] L. Vorwerk, T. Engel and C. Meinel, A proposal for combination of compression and encryption, Proceedings of Visual Communications and Image Processing, SPIE, Vol. 4067, 2000.
[20] I. Masanori, O. Noboru, A. Ayman, M. Ali, New Image Encryption and Compression Method Based on Independent Component Analysis, 3rd International Conference on Information and Communication Technologies: From Theory to Applications, April 2008.
[21] C. P. Wu and J. Kuo, Design of Integrated Multimedia Compression and Encryption Systems, IEEE Transactions on Multimedia, Vol. 7, No. 5, 2005.
[22] W. Effelsberg and R. Steinmetz, Video Compression Techniques, Heidelberg, Germany: Dpunkt-Verlag, 1998.
[23] W. Zeng and S. Lei, Efficient Frequency Domain Selective Scrambling of Digital Video, IEEE Transactions on Multimedia, 5(1), March 2003.
[24] 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.
[25] I. Agi and L. Gong, An empirical study of secure MPEG video transmission, Symposium on Network and Distributed Systems Security, 1996.
[26] M. V. Droogenbroeck and R. Benedett, Techniques for a selective encryption of uncompressed and compressed images, Proceedings of ACIVS, Ghent, Belgium, September 2002.
[27] M. V. Droogenbroeck, Partial Encryption of Images for Real-Time Applications, 4th IEEE Signal Processing Symposium, Hilvarenbeek, The Netherlands, pp. 11-15, 2004.
[28] 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.
[29] K. Hong and K. Jung, Partial Encryption of Digital Contents Using Face Detection Algorithm, Springer-Verlag, 2006.
[30] 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.
[31] 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.
[32] 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.
[33] E. N. Lorenz, The Essence of Chaos, University of Washington Press, Seattle, WA, 1993.
[34] H. S. Kellert, In the Wake of Chaos: Unpredictable Order in Dynamical Systems, University of Chicago, pp. 56-62, 1993.
[35] L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine 1(3): pp. 6 21, 2001.
[36] S. Li, Analyses and New Designs of Digital Chaotic Ciphers., PhD thesis, School of Electronics & Information Engineering, Xian Jiaotong University, Xian, China, 2003.
[37] M. S. Baptista, Cryptography with chaos, Physics Letters A 240, pp. 50-54, Elsevier Science, 1998.
[38] G. Jakimoski and L. Kocarev, Analysis of Some Recently Proposed Chaos-Based Encryption Algorithms, International IEEE conference on Multimedia, 2007.
[39] M. Sharma and M. K. Kowar, Image Encryption Techniques Using Chaotic Scheme: a Review, Int. Journal of Engineering Science and Technology, Vol.2, pp. 2359-2363, 2010.
[40] J. Fridrich, Image encryption based on chaotic maps, Proceedings of International IEEE Conference on Sysytems, Man and Cybernetics, Vol. 2, pp. 11051110, 1997.
[41] J. Fridrich, Secure image ciphering based on chaos, Technical Report RL-TR-97-155, the Information Directorate of the Air Force Research Laboratory, New York, 1997.
[42] J. C. Yen and J. In Guo, A New Chaotic Key-Based Design for Image Encryption and Decryption, IEEE International Symposium on ISCAS, Geneva, pp. 49-52, 2000.
[43] M. I. Sobhy, and A. R. Shehata, Chaotic Algorithms for Data Encryption, IEEE Proceeding of ICASSP, Vol 2, pp. 997-1000, 2001.
[44] F. Belkhouche and U. Qidwai ,Binary image encoding using 1D chaotic maps, IEEE Annual Technical Conference Region 5, 2003.
[45] Z. Han and W. X. Feng, A new image encryption algorithm based on chaos system Proc. IEEE Int. Conf. Robotics, Intelligent Systems and Signal Processing. Changsha, China, pp. 778-782, 2003.
[46] S. Deng, L. Zhang and Di Xiao, Image Encryption Scheme Based on Chaotic Neural System, Lecture Notes in Computer Science, Volume 3497, pp. 868-872, 2005.
[47] M. R. Zhang, G. C. Shao and K. C. Yi, T-matrix and its applications in image processing, IEEE Electronics Letters, Vol. 40 No. 25, 9th December 2004.
[48] Z. YiWei, W. YuMin and S. XuBang, A chaos-based image encryption algorithm using alternate structure, Science in China Series F: Information Sciences, Springe-Verlag, vol. 50, no. 3, 334-341, 2007.
[49] M. Ahmad and M. Shamsher Alam, A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping, International Journal on Computer Science and Engineering, Vol.2 (1), pp. 46-50, 2009.
[50] I. A. Ismail, M. Amin and H. Diab, A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps, International Journal of Network Security, Vol.11, No.1, PP.1-10, July 2010.
[51] G. Srividya and P. Nandakumar, A Triple-Key Chaotic Image Encryption Method, International Conference on Communications and Signal Processing (ICCSP), 2011.
[52] N. K. Pareek, Vinod Patidar, K. K. Sud; "Image encryption using chaotic logistic map", Image and Vision Computing 24 (2006) 926-934.
[53] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), pp. 191-204, Springer-Verlag, 1994.
[54] Rivest, Shamir and Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21 (2): pp. 120126, 1978.

[55] 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.
[56] T. Chen, J. Wang and Y. Zhou, Combined Digital Signature and Digital Watermark Scheme for Image Authentication, Int. Conferences on Info-tech and Info-net, Beijing, 2001.
[57] C. S. Lu and H. Y. Mark Liao, Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme, IEEE Transactions on Multimedia,Vol.5,No.2, 2003.
[58] 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.
[59] G. Zhao, X. Yang, B. Zhou and Wei Wei, RSA-based digital image encryption algorithm in wireless sensor networks, 2nd International Conference on Signal Processing Systems (ICSPS), 2010.
[60] K. Gupta, S. Silakari, Performance Analysis for Image Encryption Using ECC, Int. Conference on Computational Intelligence and Communication Networks, 2010.
[61] A. Yahya and Ayman M. Abdalla, A Shuffle Image-Encryption Algorithm, Journal of Computer Science 4 (12): pp. 999-1002, 2008.
[62] J. M. Rodrigues, W. Puech and A. G. Bors, SELECTIVE ENCRYPTION OF HUMAN SKIN IN JPEG IMAGES, International IEEE Conference on Image Processing, 2006.

Ali Soleymani received his BSc in Computer Hardware Engineering and MSc in Computer Architecture Engineering both from Islamic Azad University, Iran in 2002 and 2006 respectively. Then he was a lecturer in Islamic Azad University, Iran from 2003 to 2010 and now he is a PhD student in the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM) since 2010. His research interests include image processing, cryptography and network security.

Zulkarnain Md Ali received his BSc in Computer and Education from Universiti Teknologi Malaysia, Johor, Malaysia in 1994. He got MSc in IT from Loughborough University, United Kingdom in 1997 and he completed his PhD in Computer Network from Universiti Putra Malaysia, Serdang, Malaysia in October 2010. He is currently a Senior Lecturer in the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. He is a chairperson of Programming Research Group (ATUR) in the faculty. He is interested in the area of cryptography, parallel computing and image security. He is currently works in the image security based on public key cryptosystem.

Md Jan Nordin received both BS and MS degrees in Computer Science from Ohio University, USA in 1982 and 1985 respectively. He received PhD degree in Engineering Information Technology from Sheffield Hallam University, United Kingdom in 1995. Currently, he is an Associate Professor at School of Computer Science, National University of Malaysia (UKM). His current research interests include pattern recognition, computer vision, intelligent system and image reconstruction.