THE DILEMMA OF DIGITAL IMAGE SECURITY: AN INVESTIGATION STUDY INTO THE REQUIREMENTS AND TECHNIQUES

Hassan Alqahtani and Paul Sant
Department of Computer Science and Technology,
University Campus Milton Keynes (UCMK), Milton Keynes, U.K

ABSTRACT

Image encryption plays a paramount part to guarantee classified transmission and capacity of image over web. Then again, a real-time image encryption confronts a more noteworthy test because of vast measure of information included. This paper defines the digital image security requirements, and investigates the proposed mechanism from watermarking, steganography, and encryption algorithms. The conducted investigation aims to highlight the features, weaknesses, strengths, and limitations as well, and compare between these mechanisms in term of defined criteria.

KEYWORDS: *image encryption, cryptography, steganography, Watermarking.*

I. INTRODUCTION

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in different-different processes. Therefore, the security of image data from unauthorized uses is important. Image encryption plays an important role in the field of information hiding. Image encryption method prepared information unreadable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message or any other type of transmitted information through public networks such as internet.

Steganography, Cryptography and Watermarking are well known and widely used to hide the original message. Steganography is used to embed message within another object known as a cover work, by tweaking its properties; By using Cryptography sender convert plaintext to cipher text by using Encryption key and other side receiver decrypt cipher text to plain text. Digital watermarking is a technique for inserting information (the watermark) into an image (visible or invisible) [1].

The paper’s structure could be explained as follows: Section II summarises the security system aims. Section III discusses the image protection techniques. Next three chapters will discuss the cryptography, steganography, and watermarking; respectively. Section VII, provide a comparison between these techniques. Finally, Section VIII and Section IX will sum up the study outcomes and highlights the future work.

II. SECURITY SYSTEM AIMS

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography [2].

- Access control: Only the authorized parties have the ability to access the given information.
- Confidentiality Information in computer is transmitted and must be accessed only by the authorized party and not by anyone else.
- Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.

- Non-repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.
- Integrity: the authorized party is able to modify the data. Any alteration process must be detected by the data owner.

III. IMAGE PROTECTION TECHNIQUES

There are many security systems have been developed in order to protect and maintain specific security features; such as, integrity, safety, access control and others.[2] These systems could be classified into two main categories (The cryptography techniques, and the data hiding techniques), as Figure 1.

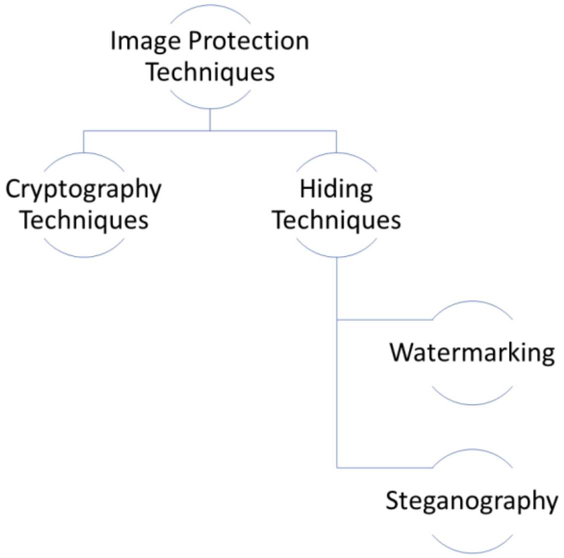

Figure 1. Image Protection techniques

The cryptography techniques depend on the cipher theory; when some mathematical equations applied to the original data in order to make in understand form. These techniques will be reviewed in section IV. The other category is the data hiding, these techniques can be divided into two type of groups, depending on the objectives of techniques. The techniques that aim to hide information inside other information via embedding these information; the second technique usually aim to stamp the information, in order to prove the information ownership [3-5]. Figure 3 illustrates the information hiding techniques based on the security system objectives.

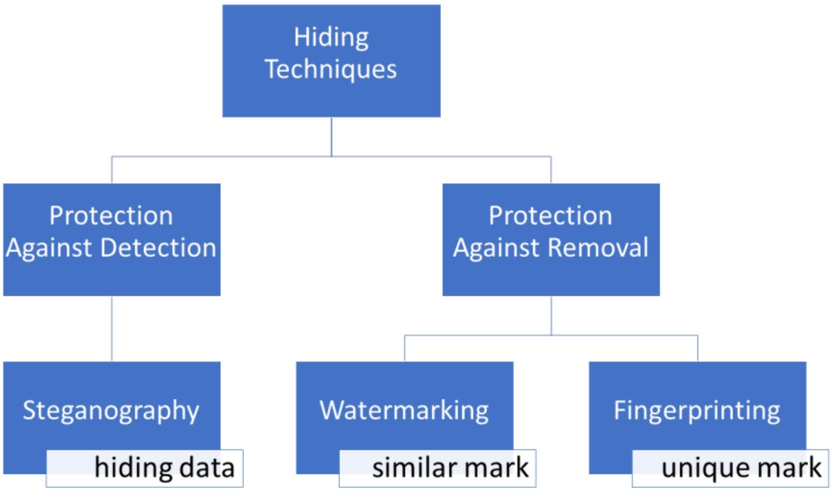

Figure 2. Image hiding techniques based on the objectives [2]

IV. CRYPTOGRAPHY

Cryptography is the science or study of techniques of secret writing and message hiding (Dictionary.com 2009). Cryptography is as broad as formal linguistics which obscure the meaning from those without formal training. It is also as specific as modern encryption algorithms used to secure transactions made across digital networks. Cryptography constitutes any method in which someone attempts to hide a message, or the meaning thereof, in some medium.

Encryption is one specific element of cryptography in which one hides data or information by transforming it into an undecipherable code. Encryption typically uses a specified parameter or key to perform the data transformation. Some encryption algorithms require the key to be the same length as the message to be encoded, yet other encryption algorithms can operate on much smaller keys relative to the message. Decryption is often classified along with encryption as it's opposite. Decryption of encrypted data results in the original data [1,7]. A cipher is an algorithm, process, or method for performing encryption and decryption. A cipher has a set of well-defined steps that can be followed to encrypt and decrypt messages. The operation of a cipher usually depends largely on the use of an encryption key. The key may be any auxiliary information added to the cipher to produce certain outputs. Technically, the cryptography approaches could be categorised into two main categories as shows into Figure 3 illustrates encryption types and their algorithms as well [8].

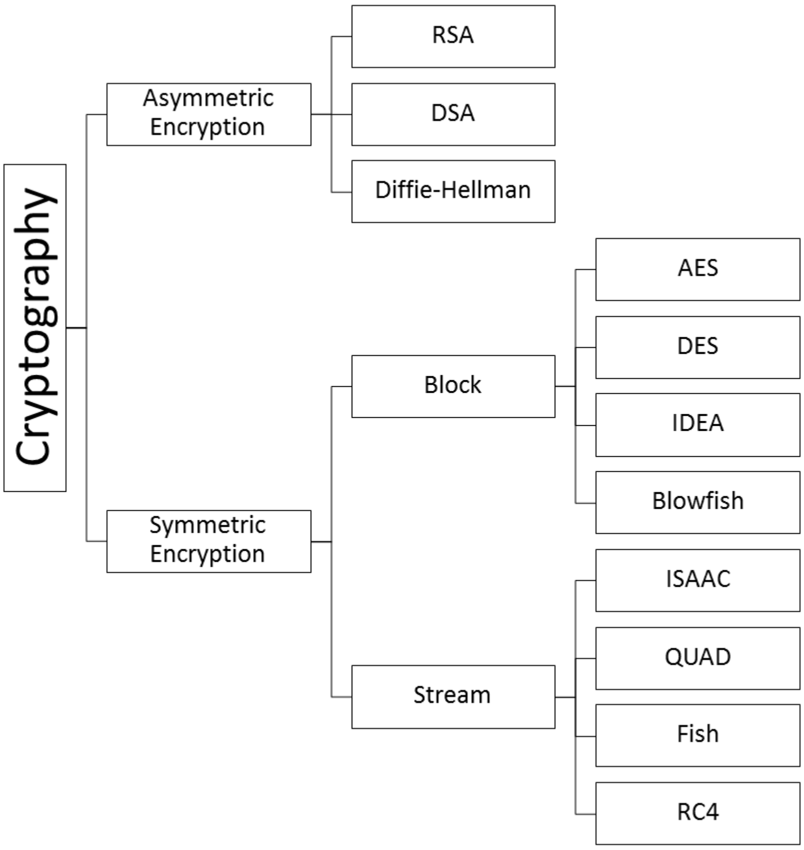

Figure 3. Cryptography Categorisation

The symmetric key, sometimes called private-key, encryption cipher is any algorithm in which the key for encryption is trivially related to the key used for decryption. An analogy of this is a typical mechanical lock. The same key that engages the lock can disengage it. To protect anything valuable behind the lock, the key must be given to each member securely. If an unintended person obtains access to the key, he or she will have full access to what is being secured by the lock. There are several modern algorithms that implement a symmetric key encryption scheme [9]. One method of symmetric key encryption is a stream cipher, where a stream of random, or pseudo- random, numbers are combined with the original message. Specific stream ciphers include: One-Time Pad, linear Feedback Shift

Register (LFSR), Liner Congruential, and RC4. RC4 is the most widely-used stream cipher and is used in Secure Socket Layer (SSL) and Wired Equivalent Privacy (WEP) [10-12].

Another method of symmetric key encryption is a block cipher, which operates on a fixed of bits. When encrypting, a block cipher takes a set amount of bits (i.e. 128 outputs a corresponding same size (i.e. 128 cipher is controlled by the encryption/decryption DES, and AES. AES is an encryption standard adopted by the U.S. government and has been approved by the National Security Agency (NSA) for encryption of "top secret" information. Many current methods of symmetric key encryption employ both stream and block schemes [1].

The RSA encryption, named for the surnames of the inventors, relies on multiplication and exponentiation being much faster than prime factorization. The entire protocol is built from two large prime numbers. These prime numbers are manipulated to give a public key and private key. Once these keys are generated they can be used many times. Typically one keeps the private key and publishes the public key. Anyone can then encrypt a message using the public key and sent it to the creator of the keys. This person then uses the private key to decrypt the message. Only the one possessing the private key can decrypt the message. One of the special numbers generated and used in RSA encryption is the modulus, which is the product of the two large primes. In order to break this system, one must compute the prime factorization of the modulus, which results in the two primes. The strength of RSA encryption depends on the difficultly to produce this prime factorization. RSA Encryption is the most widely used asymmetric key encryption system used for electronic commerce protocols [13-14].

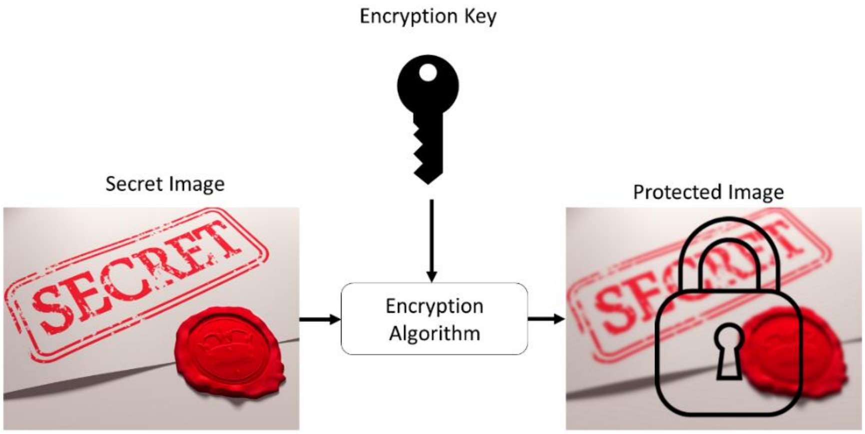

Figure 4. Encryption process

V. STEGANOGRAPHY

Steganography is derived from the Greek for covered writing and essentially means “to hide in plain sight”. According to [3] steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganography techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible. Large scale steganography, performed with computers, is typically based on human undeterminable numbers. For example, the typical audio WAV file represents one audio sample with a 16-bit number ranging from 0 to 65535 [15]. A person could split up the secret message into it bits and embed them one at a time into each audio sample, thus only changing the amplitude of the sample by 1. This means that if an actual audio sample was represented by 12345 it could only change by one. The human ear is very far from hearing this change. In this way, the secret message is put into the audio file without noticeable change and without altering the file's size. A random person would not be able to tell that an embedded message even exists. This is where the phrase "security through obscurity" comes from. An encrypted message is easily seen as encrypted and a cryptographer can begin working on decrypting it. In comparison, a message embedded into a picture, audio, or video file can pass right by without being noticed [16].

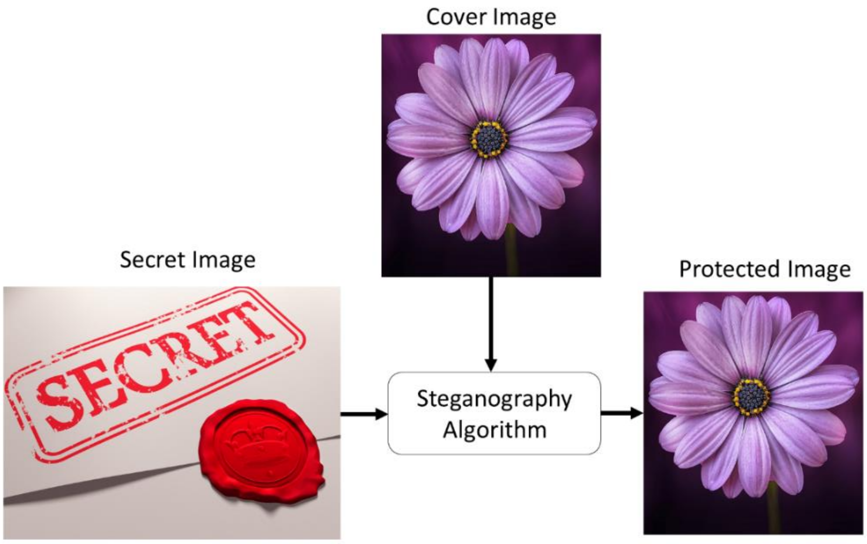

Figure 5. Steganography process

VI. WATERMARKING

Digital watermarking is a technique for inserting information (the watermark) into an image (visible or invisible). Visible water marking Decryption Key. The idea is to change the text in to format which is not easy to decrypt without decryption key, changing the alphabets with another alphabets or make a key to arrange the alphabets. Generally, organization put their logo or seal which holds rights of the organization of image [17].

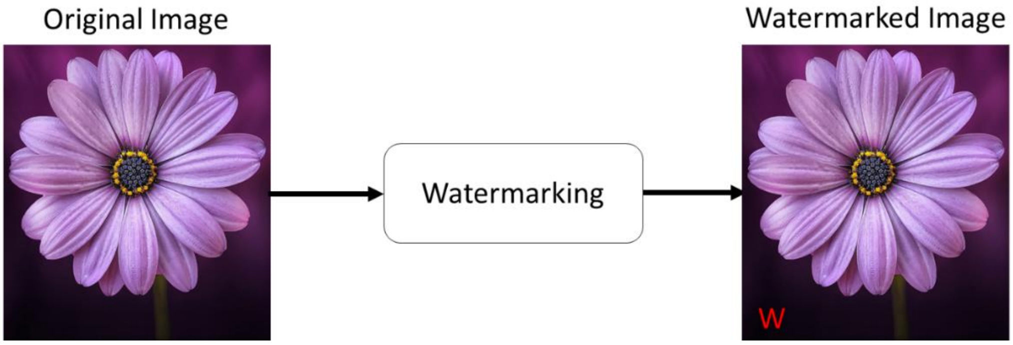

Figure 6. Watermarking process

VII. COMPARISON

Steganography and encryption are both used to ensure data confidentiality [18]. However the main difference between them is that with encryption anybody can see that both parties are communicating in secret. Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. This makes steganography suitable for some tasks for which encryption isn’t, such as copyright marking. Adding encrypted copyright information to a file could be easy to remove but embedding it within the contents of the file itself can prevent it being easily identified and removed. Steganography provides a means of secret communication which cannot be removed without significantly altering the data in which it is embedded. The embedded data will be confidential unless an attacker can find a way to detect it.

Table 1. Image protection techniques comparison

Criteria	Cryptography	Steganography	Watermarking
Authentication	Retrieve data	Retrieve data	cross correlation
Confidentiality	Yes	Yes	No
integrity	No	Yes	yes
Un-removability	Yes	Yes	no
Input	1 file	2 files	1 file
Output	Encrypted file	Stego-file	Watermarked-file
Key	Yes	Optional	No
Visibility	Always	Never	Sometimes
Application	Universal	Universal	Universal
Identification	Naked eye	No	Naked eye

VIII. CONCLUSIONS AND FUTURE WORK

To sum up, Digital watermarking is similar to a stamp which is applied on images, videos, audio, programs, or documents to prove the ownership. It is similar to the traditional watermark and is detectable only under certain conditions. Most of these digital watermarks are made invisible to the human eye but can be detected by the software. The digital watermarks have to be very robust. Illegal parties will try to remove the watermarks. Hence it is very important that the digital watermarks should be made robust. Watermark should remain unchanged even when it undergoes manipulation, copying, recording, compression, decompression, encryption, decryption, or distribution. One prerequisite is that the watermark should not affect the original content in anyway. Steganography aims to transmit secret messages through some unrelated content. The intended message is hidden inside the cover page. The latter has to be discarded by the receiver. The above two methods steganography and digital watermarking hide data. It is essential to understand at this point the difference between digital watermarking and steganography. The main aim of digital watermarking is to protect intellectual property rights and authentication of the content which is being transmitted or distributed. In digital watermarking, the watermark is always related to the content and both the content and the watermark are essential to the receiver. On the other hand, in steganography, there is no relation between the innocent looking content and the embedded secret message. The content is of no use to the receiver. The receiver has to extract the embedded secret message. Both steganography and watermarking hide data. This is different from the traditional concept of encryption where either the entire content is encrypted or an encrypted signature is added to the content. While the former restricts the free flow of the communication and also alerts hackers to the presence of encrypted data, the latter is susceptible to easy detection and removal of the encrypted signature.

IX. FUTURE WORK

It is obvious that Future work will involve further investigation to examine these challenges and provide a better understanding of the existing cryptography and steganography algorithms. The further investigation will help to develop approaches/ algorithms that capable to solve these limitations and overcome the identified obstacles.

REFERENCES

[1] ,Popa, R., 1998. “An analysis of steganographic techniques”. The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering.

[2] Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P., 2010. Digital image steganography: Survey and analysis of current methods. Signal processing, 90(3), pp.727-752.

[3] Johnson, N.F. and Jajodia, S., 1998. Exploring steganography: Seeing the unseen. Computer, 31(2).

[4] James, C., Steganography Past, Present, Future. (дата обращения: 12.12. 2009).

[5] Provos, N. and Honeyman, P., 2003. Hide and seek: An introduction to steganography. IEEE security & privacy, 99(3), pp.32-44.

[6] Sadkhan, S.B., 2004, April. Cryptography: Current status and future trends. In Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on (pp. 417-418). IEEE.

[7] Khan, M. and Shah, T., 2014. A literature review on image encryption techniques. 3D Research, 5(4), p.29.

[8] Tanaka, K., Nakamura, Y. and Matsui, K., 1990, September. Embedding secret information into a dithered multi-level image. In Military Communications Conference, 1990. MILCOM'90, Conference Record, A New Era. 1990 IEEE (pp. 216-220). IEEE.

[9] Oad, A., Yadav, H. and Jain, A., A Review: Image Encryption Techniques and its Terminologies. International Journal of Engineering and Advanced Technology (IJEAT) ISSN, pp.2249-8958.

[10] El-Emam, N.N., 2007. Hiding a large amount of data with high security using steganography algorithm. Journal of Computer Science, 3(4).

[11] Jeon, G., 2014. Watermarking Application Using Bit Plane Allocation. International Journal of Security and its Applications, 8(5), pp.139-148.

[12] Lim, Y., Xu, C. and Feng, D.D., 2001, May. Web based image authentication using invisible fragile watermark. In Proceedings of the Pan-Sydney area workshop on Visual information processing-Volume 11 (pp. 31-34). Australian Computer Society.

[13] LAKRISSI, Y., ERRITALI, M. and FAKIR, M., A comparative study of some images watermarking algorithms.

[14] Diffie, W. and Hellman, M., 1976. New directions in cryptography. IEEE transactions on Information Theory, 22(6), pp.644-654.

[15] Wong, P.W., 1998, October. A public key watermark for image verification and authentication. In Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on (Vol. 1, pp. 455-459). IEEE.

[16] Merkle, R.C. and Charles, R., 1979. Secrecy, authentication, and public key systems.

[17] Sridhar, S., 2015. A Comprehensive Approach to Image Watermarking, Encryption and Steganography. Computer and Information Science, 8(4), p.32.

[18] Cacciaguerra, S. and Ferretti, S., 2003. Data hiding: steganography and copyright marking. Department of Computer Science, University of Bologna, Italy. http://www. cs. unibo. it/-people/phdstudents/scacciag/home_files/-teach/datahiding. pdf, p.12.

[19] Atoum, M.S., Ibrahim, S., Sulong, G. and Zamani, M., 2013. A new method for audio steganography using message integrity. Journal of Convergence Information Technology, 8(14), p.35.

AUTHORS

Paul Sant joined the department of Computer Science and Technology (UoB) in September 2005 as a lecturer and he became a Senior Lecturer in September 2006. He was promoted to Principal Lecturer in August 2011. Dr. Paul completed his PhD from King's College, London in 2003 with a thesis entitled "Algorithmics of edge-colouring pairs of 3-regular trees" and prior to this, a BSc. in Computer Science from the University of Liverpool (1999). He is an active member of the British Computer Society and a Chartered Information Technology Professional (CITP) as well as being a fellow of the Higher Education Academy. In January 2013 Paul was appointed to a seconded position of Associate Dean, UCMK.

Hassan Alqahtani started his PhD March-2014 at university of Bedfordshire. His research interest includes cloud computing, mobile cloud computing, cyber security, and encryption. He received his Master degree from Teesside University in 2012, and his Postgraduate certificate from Essex University in the Telecommunication and Information System.