International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 2 Issue 12, December-2013, pp: (12-17), Available online at: www.erpublications.com

An authenticate and encrypted image using Watermark and Quantum Computing

Pawan Kumar Patel
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur, India

Abstract: The demand of security is getting higher in these days due to easy reproduction of digitally created multimedia data. Digital watermark is the emerging technique to embed secret information into content for copyright protection and authentication. Watermark is embedded within an image that alteration and modification to the watermarked image can be detected in a fragile watermark system. Watermark detection is blind that does not require an original image and it is invisible to avoid revealing secret information to malicious attackers.

Keywords: Biometrics, Watermarking, Steganography, Security, Parity Checker.

I. Introduction

In era of information technology one can observe clearly that digital information either in form of text, image, audio and, video is being transmitted and distributed unlimited number of copies through proper channel in principal[6, 7, 8]. The major challenges in doing so are protection of ownership of material, intellectual and production rights. An unauthorized person, system or device also can produce and distribute illegally number of similar copies of original copy without consent of genuine owner. These challenges lead to study ways of embedding copyright information in text, audio, video and image. Steganography and watermarking are two prominent technique to hide information in audio and video data in irremovable and/or undetectable manner.

a) Covert channels are communication paths that were neither designed nor intended to transfer information at all, but are used that way, using entities that were not intended for such use. Such channels often occur in multilevel operating systems in which security based on availability of several levels of security.
b) Anonymity is finding ways to hide meta content of the message (for example the sender and/or the recipients of the message). Anonymity is need when making on-line voting or to hide access to some web pages, or to hide sender.

A) Comparison of steganography and watermarking

The main goal of steganography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot detect the presence of m in d'.
A digital watermark is a distinguishing piece of information that is adhered to the data (generally called cover or host data) that it is intended to protect. Watermarking embeds (generally hides) a signal directly into the data and the signal becomes an integral part of the data, travelling with the data to its destination. This way, the valuable data is protected as long as the watermark is present (and detectable) in it. At any given moment, the hidden signal can be extracted to get the copyright-related information. Thus, the goal of a watermark must be to always remain present in the host data. However, in practice the requirement is somewhat weaker than that: Depending on the application, a watermark is required to survive all the possible manipulations the host data may undergo as long as they do not degrade too much the quality of the document. Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

The main goal of watermarking is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot remove or replace m in d'. It is also often said that the goal of steganography is to hide a message in one-to-one communications and the goal of

watermarking is to hide message in one-to-many communications. Shortly, one can say that cryptography is about protecting the content of messages, steganography is about concealing its very existence.

Steganography methods usually do not need to provide strong security against removing or modification of the hidden message. Watermarking methods need to be very robust to attempts to remove or modify a hidden message. A general model of a cryptographic system has already emerged.

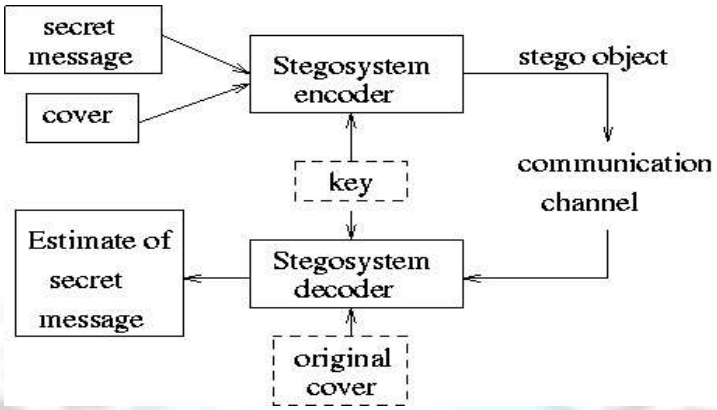


Figure 1: Model of steganographic systems

Steganographic algorithms are in general based on replacing noise component of a digital object with a to-be-hidden message. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals. One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied data.

B) Quantum and Public/Private Key cryptography

a) **Quantum Cryptography:** Cryptography is a tool that enables the secure transmission of a secret message between a sender and a recipient from any potential eavesdropper[5, 9,10,12]. Traditionally the sender is called Alice, the recipient Bob, and the eavesdropper Eve. Quantum cryptography is a particular form of cryptography that relies on the laws of quantum mechanics in order to ensure unconditional security. Traditional forms of cryptography, which are of everyday use, either rely on a public key that everybody can access or on a private key.

b) **Public key cryptography:** Public key cryptography is widely used for example by banks to perform secure money transfer, or over the Internet for securing websites access. The security of public key cryptography relies on the difficulty to realise an efficient algorithm to "crack" the communication. However these protocols are not unconditionally secure because no mathematical theorem forbids Eve to build a clever revolutionary algorithm, or a quantum computer, that will allow her to crack such codes.

c) **Private Key cryptography:** On the other hand, private key cryptography can be unconditionally secure if encryption techniques such as the 'one time pad' are performed. The weakness of these techniques is that the key has to be securely transmitted by Alice to Bob, whilst at the same time they are using cryptography because they cannot rely on their classical transmission channels.

Quantum cryptography elegantly solves this dilemma by enabling the unconditionally secure transmission of a random binary key between Alice and Bob, and hence is very often referenced as Quantum Key Distribution (QKD). Basically, the security of the transmission is ensured by the no-cloning theorem that forbids the perfect reproduction, or cloning, of a quantum system without disturbing it.

II. Quantum key distribution (QKD)

Quantum key distribution (QKD) is the first quantum information task to reach the level of mature technology, already fit for commercialization. It aims at the creation of a secret key between authorized partners connected by a quantum channel and a classical authenticated channel. The security of the key can in principle be guaranteed without putting any restriction on the eavesdropper's power.

The first two sections provide a concise up-to-date review of QKD, biased toward the practical side. The rest of the paper presents the essential theoretical tools that have been developed to assess the security of the main experimental platforms (discrete variables, continuous variables and distributed-phase-reference protocols) [13, 14, 15].

a) Encryption primitives

Encryption has been used from ancient times to protect the confidentiality of messages while they are transmitted. Today many kinds of information and communications technology (ICT) applications use a variety of encryption methods and algorithms for this goal. These include symmetric block and stream ciphers, where sender and receiver share two (identical or trivially related) keys, and asymmetric key algorithms, where two keys are related in such a way, that the private decryption key cannot easily be derived from the public encryption key[15]. Examples for symmetric key algorithms are DES, the Data Encryption Standard, and its variant Triple DES, and the currently popular Advanced Encryption Standard AES. Examples for contemporary asymmetric key algorithms are the RSA algorithm and the family of elliptic curve algorithms.

These symmetric and asymmetric algorithms have in common that the security for maintaining the confidentiality of the encrypted message is computational, i.e. it is based on the assumption that an attacker is constrained in available computing power for the attack or the available time for carrying it out. For asymmetric cryptography the security additionally depends on the assumption that no efficient algebraic method exists to reverse the utilized cryptographic functions. These assumptions require constant attention (see the web site for cryptographic key length recommendations www.keylength.com) and have in some cases required costly migration to another algorithm when their security was challenged e.g. because of the rapid increase computing power.

However, one symmetric cryptographic algorithm is different: the one time pad. If properly employed, it is the one and only information theoretically secure encryption method. Information theoretically secure refers to the fact that it can be formally proven that the amount of information an eavesdropper may have about the message is below an upper bound, which can be made arbitrarily small. The one time pad was invented in the early nineteen-twenties based on work of Gilbert Vernam and Joseph O. Mauborgne and it took almost thirty years until its 'perfect secrecy' could be proven by Claude Shannon in 1949 .For applications with highest security requirements the one time pad is still in use today, despite of its impractical prerequisites: It requires a truly random key with exactly the same length as the message to be encrypted.

b) Key distribution primitives

The generation of two identical streams of truly random bits at two distinct locations connected by a quantum channel is exactly what QKD can provide. As mentioned before, this can be achieved with information theoretically guaranteed security [1, 2, 3, 4].

Other methods for distributing secret keys make either use of a given secure channel or rely on public key cryptography. Examples for a given secure channel are the trusted courier who carries a USB flash drive filled with a random bit sequence, or a digital channel that is secured with a previously distributed secret key. In the latter case the security level for the distribution process, and hence the security level of the subsequent encryption is certainly lower than the security level of the secure channel.

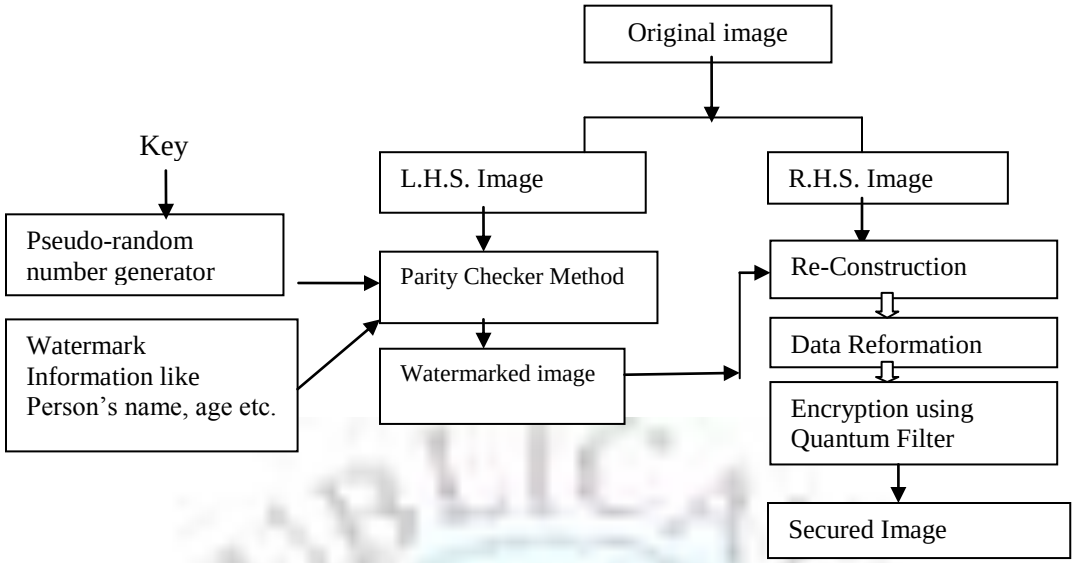


Fig 2: Process of securing biometric template

An example for a key distribution method using public key cryptography is the Diffie-Hellmann key agreement , which is e.g. used in the Secure Sockets Layer protocol (SSL/https) or in the Internet Key Exchange protocol (IKE) for setting up security associations in the IPSec protocol. In contrast to QKD, the security of both the secure channel and the public key agreement is again based on assumption. The advantage of public key distribution lies in its ability to establish a secret key between two parties without prior mutual knowledge. But it is also clear that without prior mutual knowledge the identities of the parties cannot be authenticated and a man-in-the-middle attack cannot be ruled out. The authentication of the communicating parties is usually solved with a public key infrastructure involving a trusted third party.

Quantum key distribution, too, requires authentication of the parties to rule out man-in-the-middle attacks. This is done by public discussion on the classical channel which uses a message authentication primitive to guarantee message integrity. Polarization by a filter- A pair of orthogonal filters such as vertical/horizontal is called a basis. A pair of bases is conjugate if the measurement in the first basis completely randomizes the measurements in the second basis. Sender-receiver of photons

II. Design and Implementation

In our system, we used the watermarking for security of biometric template. Biometric template can be replaced or forged by attacker. But, in our system, if attacker tries to replace or forge the biometric template then he must have the knowledge of pixel values where watermark information is hidden. If attacker changes the secure biometric template (i.e. Biometric template with watermark information) with forge biometric template then it gives the clue to database manager that something has gone wrong with biometric template because in forge biometric template either the watermark will not be present or will be present at wrong pixel positions. For the insertion of watermark information in biometric template we used the Parity Checker Method. Also, we inserted the watermark information four times in biometric template so that if attacker is able to change watermark at one place, the watermark at other places remain intact. The process of securing the biometric template is shown in Figure 2.

Algorithm

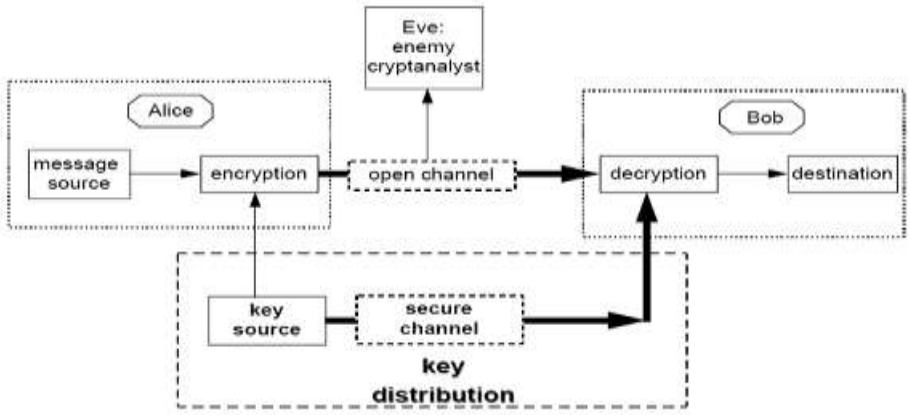
Step 1: Read the watermark information that we want to hide in the biometric template.
Step 2: Read the biometric template
Step 3: Find out the pseudorandom pixel location in the biometric template where watermark is to be inserted by using pseudorandom number generator which is seeded with the secret key.
Step 4: If at a pixel location we want to hide 0, then go to step 5 else go to step 6.

Step 5: a) Check whether there exists odd parity at the selected pixel location, then insert 0 at the pixel location (no change in pixel value is required in this case). Go to END.
b) If even parity exists, then make the odd parity at that location by adding or subtracting 1 to that pixel location (change in pixel is required in this case). Go to END.
Step 6: a) Check whether there exists even parity at the selected pixel location, then insert 1 at the pixel location (no change in pixel value is required in this case). Go to END.
b) If odd parity exists, then make the even parity at that location by adding or subtracting 0 to that pixel location (change in pixel is required in this case). Go to END.
Step 7: Merge or Re-Join watermarked image and R.H.S. Image.
Step 8: Perform Permutation with a fixed Matrix.
Step 9: Apply Encryption using BB84 security protocol using photon polarization idea.

Example: Both Alice and Bob have two polarizers each.

One with the 0-90 degree basis (+) and one with 45-135 degree basis (X)
(a) Alice uses her polarizers to send randomly photons to Bob in one of the four possible polarizations 0, 45, 90,135 degree.
(b) Bob uses his polarizers to measure each polarization of photons he receives.

He can use the (+) basis or the (x) but not both simultaneously.



Alice is going to send Bob a key.

Bit	0	1	0	1	1
Basis	+	×	×	+	×
Photon					

Bob receives the photons and must decode them using a random basis. Alice and Bob talk on the telephone:

Alice chooses a subset of the bits (the test bits) and reveals which basis she used to encode them to Bob. Bob tells Alice which basis he used to decode the same bits. Where the same basis was used, Alice tells Bob what bits he ought to have got.

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon					
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

As long as no errors and/or eavesdropping have occurred, the test bits should agree. Alice and Bob have now made sure that the channel is secure. The test bits are removed. Alice tells Bob the basis she used for the other bits, and they both have a common set of bits: the final key.

Conclusion

This work presents how watermarking helps in security of biometric template. We showed that watermarking avoids the forging and replacement of biometric template by the attacker. But, this process also increases the responsibility of database manager. Database Manager has to manage the key secretly. In future, we will try to combine watermarking with cryptography techniques and try to increase robustness of biometrics systems. We will also try to prevent other types of attacks on the biometrics systems by using watermarking, cryptography and data hiding techniques. Quantum cryptography is a major achievement in security engineering. As it gets implemented, it will allow perfectly secure bank transactions, secret discussions for government officials, and well-guarded trade secrets for industry!

The main difference between watermarking and encryption is that encryption disguises the data and protects it by making it unreadable without the correct decryption key, while watermarking aims to provide protection in its original viewable/audible form. Watermarking, like cryptography, needs secret keys to identify legal owners. The key is used to embed the watermark, and at the same time to extract or detect it. Only with a correct key can the embedded signal be revealed. While a single bit of information indicating that a given document is watermarked or not is sufficient sometimes, most applications demand extra information to be hidden in the original data. This information may consist of ownership identifiers, transaction dates, logos, serial numbers, etc., that play a key role when illegal providers are being tracked.
Watermarking can be used mainly for owner identification (copyright protection), to identify the content owner; fingerprinting, to identify the buyer of the content; for broadcast monitoring to determine royalty payments; and authentication, to determine whether the data has been altered in any manner from its original form.

References

[1]. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J., "Experimental quantum cryptography", Journal of Cryptology, vol. 5, no. 1, 1992, pp. 3 - 28. Preliminary version in Advances in Cryptology - Eurocrypt '90 Proceedings, May 1990, Springer - Verlag, pp. 253 - 265.
[2]. Bennett, C. H., Brassard, G., Crépeau, C. and Skubiszewska, M.-H., "Practical quantum oblivious transfer", Advances in Cryptology | Crypto '91 Proceedings, August 1991, Springer - Verlag, pp. 351 - 366.
[3]. Brassard, G., Crépeau, C., Jozsa, R. and Langlois, D., "A quantum bit commitment scheme provably unbreakable by both parties", Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, November 1993, pp. 362 - 371.
[4]. Barnett, S. M. and Phoenix, S. J. D., "Information-theoretic limits to quantum cryptography", Physical Review A, vol. 48, no. 1, July 1993, pp. R5 - R8.
[5]. Werner, M. J. and Milburn, G. J., "Eavesdropping using quantum-nondemolition measurements", Physical Review A, vol. 47, no. 1, January 1993, pp. 639 - 641.
[6]. Barnett, S. M., Huttner, B. and Phoenix, S. J. D., "Eavesdropping strategies and rejected-data protocols in quantum cryptography", Journal of Modern Optics, vol. 40, no. 12, December 1993, pp. 2501 - 2513.
[7]. Ekert, A. K., Huttner, B., Palma, G. M. and Peres, A., "Eavesdropping on quantum cryptosystems", Physical Review A, submitted.
[8]. Wallich, P., "Quantum cryptography", Scientific American, May 1989, pp. 28 - 30.
[9]. Deutsch, D., "Quantum communication thwarts eavesdroppers", New Scientist, 9 December 1989, pp. 25 - 26.
[10]. Flam, F., "Quantum cryptography's only certainty: Secrecy", Science, vol. 253, 1991, page 858.
[11]. Delahaye, J.-P., "Cryptographie quantique", Pour la Science, August 1992, pp. 101 - 106.
[12]. Crépeau, C., "Cryptographic primitives and quantum theory".
[13]. M.A. Dorairangaswamy Protecting Digital-Image Copyrights: A Robust and Blind Watermarking Scheme In IEEE Vol.:9, No. 4, pp. 423-27, (2009).
[14]. Feng Liu, Yongtao Qian*" A Novel Robust Watermarking Algorithm Based On Two_Levels DCT and Two_Levels SVD' Third International Conference on Measuring Technology and Mechatronics Automation IEEE pp. 206-209, (2011).
[15]. Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dual-wrapped digital watermarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, pp. 319-330, (2007).