Watermark Stamping in Digital Media

Sallauddin Khan[1*], Ravi Dubey[2], Aman Chaudhary[3], Hanamant B. Sale[4]

[1,2,3]*Student, Dept. of Information Technology, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India*

[4]*Professor, Dept. of Information Technology, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India*

*Corresponding author: pareshmhatre1901@gmail.com

***Abstract*: In traditional method of watermarking which is physically visible, there are two major concerns and those are watermark removal and unauthorized insertion. To overcome this problem, insertion of invisible watermark technique which is based on Elliptic Curve Cryptography and Sobol Sequence (Random Sampling). In the digital image watermarking system, the information carrying watermark gets embedded in the object, the object may be an image, audio or video. Image as object have been used in this paper. Digital watermarking is implemented with the help of java platform. Digital signal patterns are placed into digital images, since each image copy is combined with digital signal, this digital watermark is also called as digital signature. In present digital media security, digital watermarking is the widely used technique for protecting copy right for images or audio and video files.**

***Keywords*: Invisible-Watermarking, Digital Watermarking, Steganography, Cryptography, Watermark-Stamping.**

1. Introduction

Digital Watermarking is a method of concealing digital information in a digital message (image, audio or video) which doesn’t have any association to message and that cannot be easily extracted from the third party. Digital watermarking was first uncovered by Charles Osborne and Andrew Tirkel in 1992. The first Watermark was initiated in 13th century.

With increasing use of internet ownership proof, data validation, prevention of duplication of data, data hiding has turned to a vital issue. Data security is a prime concern for reliable communication. Cryptographic techniques are used for providing the information security but it has some limitation. To overcome the downsides of cryptography, digital watermarking technique is used.

Digital watermarking is just about similar to the steganography because in both techniques information is embedded in the digital image. In both the techniques there are negligible amount of degradation of image. The dissimilarity between these methods also known as techniques are that in steganography hidden data is only having top priority for sender and receiver but in watermarking the hidden image and the cover image both have top priority.

The Digital Watermarks can be further classified into two different types,

1. Visible watermarks
2. Invisible Watermarks

Visible watermarks can easily identify and these watermarks are not robust against image processing operation whereas invisible watermarks are more robust and secure than visible watermarks.

2. Related Work

Numerous watermarking algorithms have been offered by researchers to preserve the originality and probity of networked digital multimedia contents. Invisible-vigorous watermarking of digital images is one of the principal research areas. In this segment, we talk about the selected predominant contributions from the existing literature. One of the premature performance by Cox et al. [Cox et al. 1997] uses the technique called spread spectrum to embed a watermark in the DCT domain. To tweak this technique, Lu et al. [Lu et al. 1999] utilized a cocktail watermark to tweak lustiness and HVS to preserve high fidelity of the watermarked image. Langelaar and Biemond [Langelaar et al. 1999] offer a conclusion to implant a bit sequence in a digital image by selective removal in-stead of moderation or modification of DCT coefficients in smooth regions. This methodology may also conclude that visual artifacts. Fei et al. [Fei et al. 2004] scrutinize the accomplishment of block-based watermarking programme in the existence of lossy compression. A hybrid watermarking algorithm that has greater resilience to JPEG compression has been presented.

3. Problem Statement

The desire for availability of information and quick distribution has been a major factor in the development of new technology in the last decade. There has been tremendous increase in the use of multimedia across the internet. Distribution of multimedia has become an important way to deliver services to people all over and around the world. And due to the increase in the usage of multimedia content over the internet, some serious issues have emerged. Fraud, Counterfeiting, Forgery, and Pirating of the contents are rising. Anyone virtually with a video frame grabber, Sound Card, Scanner or multimedia authoring systems allows them to incorporate an owned or previous copyrighted material into web designs, presentation and Internet Marketing Campaigns. Consequently, copyright abuse is getting rampant among multimedia users who gets rarely caught. This copyright abuse is the motivating factor in developing new technologies. One such technology is Digital Watermarking. The focus of this proposed report will detail watermarking for multimedia applications. The regions which will be unclosed are definition of Digital watermarking, purpose, techniques and variety of watermarking attacks.

4. Methodology

There are two types of watermarking systems. The difference between them is in the nature and combination of inputs and outputs: Private watermarking systems require at least the original image and the watermark itself to detect the presence of the watermark. Public watermarking will use here, which remains the most challenging since it neither requires the original image nor the embedded watermark. This system extracts the watermark from the marked image. In this report, watermarking scheme consists of watermark embedding and watermark extracting. The cryptograph procedure is delineated in Figure 1, whereby the watermarking will be embedded / encoding process is delineated in Figure 1, whereby the watermarking will be embedded (encoded) into host image either for transparent or invisible as well as visible watermarking. Watermarked image and key file will be achieved.

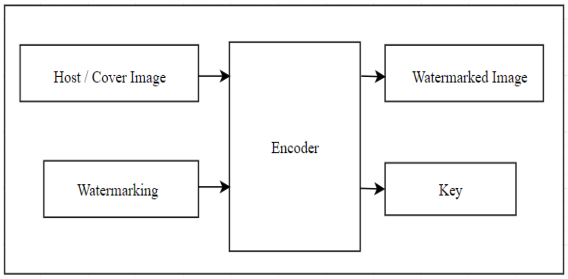

Fig. 1. Watermark Embedding

The Decoding step conversely requires reading the watermarked image and the key file to extract the watermarking. The watermark will be extracted by using the same key which was used in the embedding (encoding) stage. The decoding process is outlined in Figure 2 The proposed technique extracts the watermark from the marked image only without the original one.

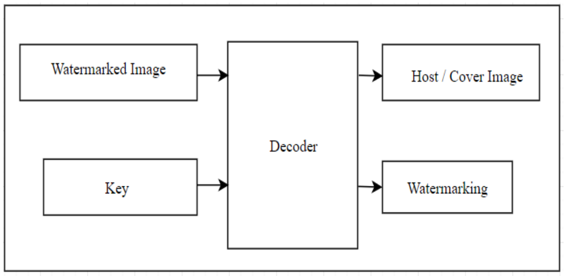

Fig. 2. Watermark Detection

5. System Architecture

A. *Overview of System Architecture*

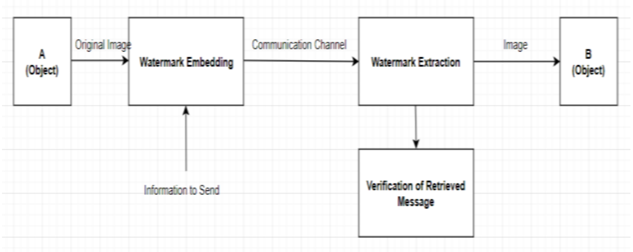

Fig. 3. Architecture Diagram

Main components are:

1) Object (Image, Voice or Video)
2) Watermark Embedder
3) Watermark Extractor
4) Appropriate Tool

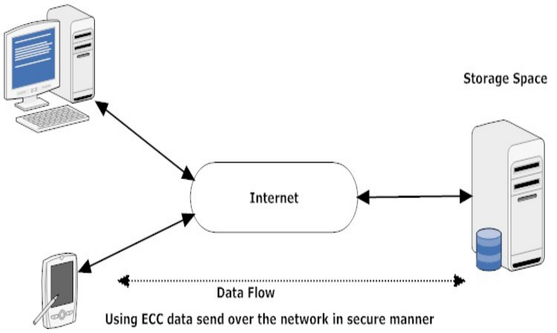

Fig. 4.

B. *Cryptography*

Cryptography or cryptology (from Ancient Greek), is the practice and as well as the study of techniques used for secure communication in the presence of third parties called adversaries. More generally, cryptography is all about constructing/creating and analyzing protocols that prevent third parties or the attackers from reading the private messages. Contemporary cryptography exists at the convergence of the regulations of communication science, computer science, mathematics, electrical engineering and physics. Military communications, electronic commerce, chip-based payment cards, digital currencies and computer passwords are the various examples or applications of cryptography

The important elements in a cryptosystems are:

a) Plain text (input)
b) Encryption algorithm
c) Secret key
d) Cipher text
e) Decryption algorithm

Plain text: Basically the plain text is an original piece of information/text, which is needed to send information to the destination.

Encryption algorithm: This is said to be the main key of any cryptographic system. And this encryption algorithm addresses the plain text to various transformations and substitutions.

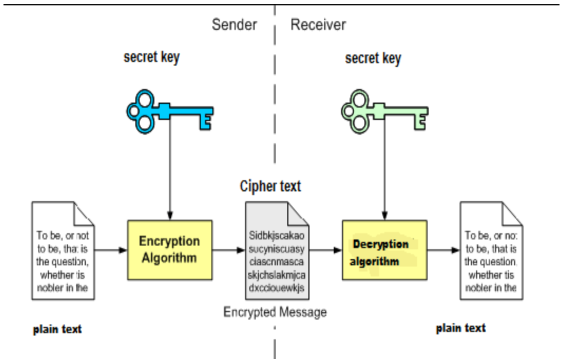
Sender
Receiver
secret key
secret key
Cipher text
To be, or not to be, tha: is the questi:n, whether :is nobler in the
Encryption Algorithm
Sidbkjscakao sucyniscuasy ciascnmasca skjchslakmjca dxccioueWkjs
Decryption algorithm
To be, or no: to be, that is the question, whether tis nobler in the
Encrypted Message
plain text
plain text

Fig. 5. General model of cryptographic system

Secret key: The secret key is particularly given by the user/sender which will act as an input to the encryption algorithm. And based on this key, various transformations and substitutions on the plain text will differ.

Cipher text: This can be called as the output generated by the encryption algorithm. The cipher text is nothing but the jumbled text. The cipher text differs with each and every secret key that has been given to the encryption algorithm.

Decryption algorithm: This is generally the opposite to the "encryption algorithm". It will acquire cipher text and secret key as an input and will produce plain text as a final output.

6. Analysis

General or public key encryption methodology is an elliptical curve cryptography (ECC) based on elliptic curve hypothesis that can be utilized to create faster, smaller, and more efficient cryptographic keys. The ECC which is Elliptical Curve Cryptography produces the keys through the characteristics of elliptic curve equation rather than the traditional method of generation. And because as ECC helps to establish equivalent security which comes with lower battery resource usage and computing power, and it is also becoming widely used for mobile applications. ECC which is Elliptical Curve Cryptography was evolved by Certicom, which is a Mobile E-business security provider, and was lately licensed by the Hifn, which is a producer of unified circuitry also commonly known as Integrated Circuitry (IC) and products related to network security. The properties & the functions of elliptic curves have been studied in mathematics branch from almost last 150 years. The utilization of ECC which is Elliptical Curve Cryptography within cryptography was firstly proposed in the year 1985, from the University of Washington by Neal Koblitz and Victor Miller at IBM(separately). An elliptic curve is not an ellipse (oval shape), but is used to constitute a looping line intersecting two axes. ECC is basically based on the properties of a particular type of equation created from the mathematical group (a set of values for which the operations can be performed on any two members of the group to produce the third member) derived from points where the line intersects the axes. Accumulating a point on the curve by a number will assemble another point on the curve, but it is extremely hard to search what number was being used, even if you know the original point and the conclusion or the result. The Equations which is based on elliptic curves have a property that is very important or valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse.

1. Smaller keys or Shorter keys are as powerful as long key for RSA.
2. Low on CPU consumption.
3. Low on memory usage.
4. Size of encrypted data is smaller

In modern world ECC i.e. elliptical curve cryptography algorithm is utilized in case of key exchanges by certificate authority (CA) to share the public key certificates with end users. The ECC i.e. Elliptic Curve Cryptography is a safe, secure and more efficient encryption algorithm rather than RSA as it utiilzes shorter key sizes for same level of security as compared to RSA. For example, a 256-bit ECC i.e. Elliptic Curve Cryptography public key imparts comparable security to a 3072-bit RSA public key. The main objective of this work is imparting an insight into the utilization of ECC i.e. Elliptic Curve Cryptography algorithm for data encryption before uploading the documents on to the cloud. ECC i.e. Elliptic Curve Cryptography was found and discovered in 1985 by Neil Koblitz (University of Washington) and Victor Miller (IBM) as a revolutionary mechanism for implementing public-key cryptography. Public-key algorithms generate a contrivance for sharing keys among big numbers or large numbers of participants or entities in a complex information system. Unlike other famous and most popular algorithms such as RSA, ECC is totally based on discrete logarithms that are much more hard and difficult to challenge at equivalent key lengths. Each and every contributor in the public key cryptography will have two keys, a pair of keys, a public key and private key, utilized for encryption and decryption operations. As the public key is generally distributed to all the participants where as private key is only known to the particular participant only.

7. Conclusion

The big and huge need of networked multimedia system has created the urgent need for protection of copyright, so it is very important to protect intellectual properties of digital media. For this Watermark Stamping is the great solution for the protection of legal rights of digital content.

In this report the survey of digital watermarking, its framework, their requirements and applications are presented. Apart from it there is a brief and comparative discussion on the various techniques of the digital image watermarking along merits and demerits. We also discuss about its classification with the aspects of documents, domain, robustness and perceptivity. In order to implement the techniques of watermarking one should examine the specific purpose for which digital multimedia is watermarked. In the digital watermarking techniques the emphasis is on fragile and robust watermarking because the watermark in the robust watermarking are designed in such a way that it can be detected even after a various attempts made for the removal of watermark and in fragile watermarking watermark brings for the purpose of authentication of the digital data.

References

[1] Purnima Pal, "Study on Watermarking Techniques in Digital Images."

[2] A Robust Double-Blind Secure High Capacity Watermarking and Information Hiding Scheme for Authentication and Tampering Recovery Via the Wavelet and Arnold Transforms

[3] S. Swapnil and D. B. Megherbi, "Center for Computer Man/Human Intelligence Networking and Distributed Systems (CMINDS)."

[4] Minewa M. Yeung and Fred Mintzer, "An Invisible Watermarking Technique for Image Verification."

[5] Elliptic curve cryptography, https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[6] RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm)

[7] JavaTM Cryptography Extension (JCE), Reference Guide. http://docs.oracle.com/javase/1.5.0/docs/guide/security/jce/JCERefGuide.htm