International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 04
April 2019

Digital Watermarking and Encryption: A Review

Reenu Rani & Neeraj

[1]Department of Computer Science & Engineering
PM College of Engineering Kami, Sonepat
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
[1]reenukundu31@gmail.com

[2]Department of Computer Science & Engineering
PM College of Engineering Kami, Sonepat
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
[2]neerajlakra5@gmail.com

Abstract— *Digital Watermarking also referred to as simply watermark is a pattern of bits inserted into a digital image, audio, video or text file that identifies the file's copyright information (author, rights, etc.). The name comes from the faintly visible watermarks imprinted on stationary that identify the manufacturer of the stationery. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. Digital watermarking can be characterized on the basis of several properties which depend on the type of application. These properties include robustness, capacity, imperceptibility, security and other restrictions. The art of securing information by scrambling it into unrecognizable format called cipher text. A secret key is used for encryption and decryption process. Cryptography only hides the content of message not the existence of message. In this paper we provide a review on various digital watermarking & encryption techniques.*

Keywords— Digital watermarking, Cryptography, Encryption & Decryption, Copyright Protection.

I. INTRODUCTION

Digital watermarking [1] is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format.

Digital Watermarking also referred to as simply watermark is a pattern of bits inserted into a digital image, audio, video or text file that identifies the file's copyright information (author, rights, etc.). The name comes from the faintly visible watermarks imprinted on stationary that identify the manufacturer of the stationery. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format [2].

We can understand the need for digital watermarking by using following paragraphs.

Suppose a person X creates an Image and publish it on the web. A person Y with bad intentions steals the Image, maybe modify it little bit and then start selling, as it was his own. X notices that Y is selling his Image. But how can he prove that he is really the owner and make Y to pay him a lot of money?

Many solutions are there to solve this problem like digital signatures. But these solutions need additional bandwidth. So, Due to limitations of the traditional copyright protection system, a new technique came in existence. This technique is known as digital watermarking. Figure 1 below shows the need for digital watermarking.

Figure 1: Need for digital watermarking

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 04
April 2019

The art of securing information by scrambling it into unrecognizable format called cipher text [3]. A secret key is used for encryption and decryption process. Cryptography only provides security by encryption and decryption. However, encryption cannot help the seller monitor how a legitimate customer handles the content after decryption. So there is no protection after decryption. Unlike cryptography, watermarks can protect content even after they are decoded. In this paper we provide a review on various digital watermarking & encryption techniques.

II. Applications of Digital Watermarking

Digital watermarking is used for the protection of ownership rights of digital media, like images, video, audio, and other multimedia objects. It can be applied to various applications such as content authentication, copyright protection, copy control, owner identification and secret communication.

The main applications of digital watermarking are listed below [4]:

1) Copyright Protection

For intellectual property protection and copyright, the copyright data can be added into the new production as a watermark. Where, the watermark can be extracted to give the information about owner of this product. Copyright applications should be imperceptible, require a high degree of robustness and but may have low capacity.

2) Content Authentication

The objective of authentication applications is for detecting any modifications of the data. In other words, the digital watermark contains data which can be used for proving that the digital content has not been changed. This can be achieved with fragile watermarks which have a low robustness to certain attacks such as compression, but are destroyed by other attacks.

3) Owner Identification

The owner identification data can be embedded into image as a watermark that is a visual or visible watermark (traditional form). However, this can be overcome using some programs which modify the images. In order to overcome the problem, invisible watermarks are used.

III. Literature Review

Various types of digital watermarking & encryption techniques are available. In this section, we provide the literature review of work done in this field.

Chunlin Song et. al. [5] described that "The aim of digital watermarking is to include subliminal information in multimedia information to ensure a security service or simply a labeling application. It would be then possible to recover the embedded message at any time, even if the information was altered by one or more non-destructive attacks, whether malicious or not. Its commercial applications range from copyright protection to digital right management. This paper then classifies the different watermarking techniques into several categories depending upon the domain in which the hidden data is inserted; the size of the hidden data and the requirement of which the hidden data is to be extracted, an experiment is conducted to further test the robustness of some of these techniques. At the end, this paper analyses challenges that have not been met in current watermarking techniques".

Peter GOČ-MATIS et. al. [6] described "a new method for video watermark embedding, using the knowledge's already available from watermark embedding into digital static pictures. The watermark is embedded in transformed domain using Discrete Wavelet Transform (DWT). This paper also describes experiments conducted on the proposed watermark embedding method. The goal of these experiments was the test the robustness of the method presented in the paper against several watermarking attacks."

Z. J. XU et. al. [7] described that "The technology of image watermark is very important in the field of signal processing. The knowledge of image watermark as well as the DCT/IDCT had been introduced in this paper. A new digital watermarking encryption algorithm had been introduced which the watermarking information was based on the size of the image. The watermark's embedding and extraction had been performed on two images for verifying this watermarking algorithm by MATLAB, and the result show that the adaptive algorithm is effective".

Ma Bin [8] wrote that "The digital watermark is scrambled with logistic chaotic sequences to improve the security of the system. Then the watermark signals are converted into a binary sequence embedded to the high (HL and HH) frequency band of the document in DWT domain. The algorithm of how to embed and extract the watermark is shown in the paper. Image quality is checked with a number of widely used

parameters such as PSNR, Normalized correlation and JPEG compression. The experimental results demonstrate the efficiency of the proposed scheme, which is practicality perfect by means of good balance between transparency and robustness".

Manoj Ramaiya et. al. [9] in their paper described "a new robust watermarking technique for color images was performed. In this paper, the RGB image is converted to HSV and watermarked by using discrete wavelet transform. Watermarking embedded stage and extraction stage is designed using another low power invisible watermarking algorithm. In this, the host signal is an image and after embedding the secret data a watermarked image is obtained and then extracts secret image and original image separately. In future the resulted watermarked image was tested with several attackers to verify the robustness and VLSI implementation of invisible watermarking algorithm using VHDL code and also check various performances like power, PSNR and tamper detection and area".

Chen Li et. al. [10] wrote a paper "Wavelet Bases and Decomposition Series in the Digital Image Watermarking that analyzes and compares the performance of different wavelet bases in the digital image watermarking and the effect of different wavelet decomposition series for the digital image watermarking embedding based on the application of wavelet in the digital image watermarking. The experiments proved the digital image watermarking embedding based on bi-orthogonal wavelet better than others".

Xiong Shunqing et. al. [11] proposed "a new algorithm of digital watermarking based on combining the Non Sub Sampled Contourlet Transform and SVD, they first applied the NSCT to the image and extract the low-frequency sub-band of image, and then decompose the low-frequency sub-band of image by SVD, finally embed the watermarking in the decomposed singular value. The experiment results show that the new algorithm has good ability in standing up to geometric attacking, especially rotation attacks."

Baiying et.al [12] in their paper proposed "A robust audio watermarking scheme based on LWT-DCTSVD, DWT-DCT-SVD with exploration of DE optimization and DM quantization. The attractive properties of SVD, LWT/DWT-DCT, DE and quantization technique make our scheme very robust to various common signal processing attacks. Meanwhile, the proposed scheme is not only robust against hybrid and de-synchronization attacks, but also robust against the Starmark for audio attacks. The experimental results validate that the proposed watermarking scheme has good imperceptibility too. The comparison results with other SVD-based and similar algorithms indicate the superiority of scheme".

Sasmita Mishra et. al. [13] presented "a comprehensive survey on various digital watermarking techniques their requirements and applications. The use of different type of watermark is application dependent. But there are neither type of watermarks are ideal when considering information preserving transformations that preserve the meaning of the content & information altering transformations that change the expression of the content. To solve this problem a semi fragile watermark is for images which can detect the information altering transformations even after the watermarked contents are subjected to information preserving alterations have to be used".

Y. Shantikumar Singh et. al. [14] in their paper "have reviewed some recent algorithms, proposed a classification based on their intrinsic features, inserting methods and extraction forms. Many watermarking algorithms are reviewed in the literatures which show advantages in systems using wavelet transforms with SVD. In this paper they also have presented a review of the significant techniques in existence for watermarking those which are employed in copyright protection. Along with these, an introduction to digital watermarking, properties of watermarking and its applications have been presented. In future works, the use of coding and cryptography watermarks will be approached".

Vinita Gupta et. al. [15] surveyed the paper on digital image watermarking. "They also classified the watermarking techniques based on the transform domain where the watermark is embedded. Also, explain the watermarking properties, applications and techniques used. This paper also shows the different techniques and discusses the important technology called QR code which can be used in future work".

Ali Moradmard et. al [16] described that "protection of information plays an essential role in message exchange and trading. Encryption is used to meet the security needs of safe transaction. Regarding the importance of the issue and the shift of traditional stage to digital stage, familiarity with encryption methods seems necessary. Different data have different methods of encryption. Images are also one type of data for which encryption is critically needed to prevent impermissible access. In this article, first a primary image is selected, then, based on the proportion of the image needing encryption, pixels

from code image are picked and is being encrypted by a function. In the next stage, this proportion is being XOR-ed by the pixel proportion of the image needing encryption, and eventually the final proportion is encrypted by Hill Algorithm. At the end, maintaining the image quality after decryption is evaluated by standards such as PSNR and SSID".

Jai Singh et. al. [17] described that "Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. In this work they encrypted and decrypted digital images by using symmetric key cryptography using MATLAB".

Majdi Farag Mohammed El Bireki et. al. [18] had adopted a digital watermarking technique which operates in the frequency domain: a hybrid watermarking scheme based joint discrete wavelet transform – discrete cosine transform – (DWT-DCT). Its main objective is to test whether this technique can withstand attacks (its robustness) and invisibility (its imperceptibility), achieved by taking DCT of the DWT coefficients of the LL mid-frequency sub-bands from its band. To ensure security, the secret code (watermark) is scrambled using the Arnold transformation which is embedded in the original host image; only gray-scale digital images are used. The results of this research reveal that the secret code (watermark) is strong enough against threats (noise). Comparative results are measured using signal-to-noise ratio criterions, mean square error and normalized cross correlation".

IV. CONCLUSION

Digital watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format. The art of securing information by scrambling it into unrecognizable format called cipher text. A secret key is used for encryption and decryption process. Cryptography only provides security by encryption and decryption. However, encryption cannot help the seller monitor how a legitimate customer handles the content after decryption. So there is no protection after decryption. Unlike cryptography, watermarks can protect content even after they are decoded. In this paper we provide a review on various digital watermarking & encryption techniques.

REFERENCES

[1] "Digital Watermarking" available at http://en.wikipedia.org/wiki/Digital_watermarking.

[2] Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" submitted at University Salzburg, pp. 9 – 17, Jan 2000.

[3]. Prabhsimran Singh, Sukhmanjit Kaur, Sabia Singh, "Cryptography: An Art of Data Hiding", Prabhsimran et al, / International Journal of Computer and Communication System Engineering (IJCCSE), Vol. 2 (1), 2015, 117-120. ISSN: 2312-7694

[4] Chauhan Usha, Singh Rajeev Kumar, "Digital Image Watermarking Techniques and Applications: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016.

[5] Chunlin Song, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images", ISBN: 978-1-902560-22-9 © 2009 PG Net.

[6] Peter GOČ-MATIS, Tomáš KANÓCZ, Radovan RIDZOŇ, Dušan LEVICKÝ, "Video watermarking based on DWT", SCYR 2010 - 10th Scientific Conference of Young Researchers, 2010.

[7] Z. J. XU, Z. Z.WANG, Q.LU, "Research on Image Watermarking Algorithm based on DCT", 3rd International Conference on Environmental Science and Information Application Technology (ESIAT 2011), © 2011 Published by Elsevier Ltd.

[8] Ma Bin, "Experimental Research of Image Digital Watermark Based on DWT Technology", 2011 International Conference on Uncertainty Reasoning and Knowledge Engineering, ©2011 IEEE.

[9] Prof. Manoj Ramaiya Richa Mishra, "Digital Security using Watermarking Techniques via Discrete Wavelet Transform", National Conference on Security Issues in Network Technologies August 11-12, 2012.

[10] Chen Li, Cheng Yang, Wei Li, "Wavelet Bases and Decomposition Series in the Digital Image Watermarking", Advances in Intelligent and Soft Computing, Advances in Multimedia, Software Engineering and Computing Vol.2 , s.l. : Springer, 2012.

[11] Xiong Shunqing, Zhou Weihong, Zhao Yong, "A New Digital Watermarking Algorithm Based on NSCT and SVD", Advances in Control and Communication, LNEE, 2012.

[12] Baiying Lei, Ing Yann Soon, and Ee-Leng Tan, "Robust SVD-Based Audio Watermarking Scheme with Differential Evolution Optimization", IEEE Transactions On Audio, Speech and Language Processing, Vol. 21, No. 11, November 2013.

[13] Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh, "A Review of Different Techniques on Digital Image Watermarking Scheme", International Journal of Engineering Research, ISSN: 2319- 6890, Volume No.2, Issue No.3, pp:193-199, 01 July 2013.

[14] Sasmita Mishra, Amitav Mahapatra, Pranati Mishra "A Survey on Digital Watermarking Techniques", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3), 2013, 451-456.

[15] Vinita Gupta, Atul Barve, "A Review on Image Watermarking and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 4, Issue 1, January 2014.

[16] Ali Moradmard, Mohammad Tahghighi Sharabiani, "Color image encryption by code image and hill algorithm", International Journal of Intelligent Information Systems 2014; 3(6-1): 98-102.

[17] Jai Singh, Kanak Lata and Javed Ashraf, "Image Encryption & Decryption with Symmetric Key Cryptography using MATLAB", International Journal of Current Engineering and Technology, Vol.5, No.1 (Feb 2015).

[18] Majdi Farag Mohammed El Bireki, M. F. L. Abdullah, Ali Abdrhman M. Ukasha and Ali A. Elrowayati, "Digital Image Watermarking Based on Joint (DCT-DWT) and Arnold Transform", International Journal of Security and Its Applications Vol. 10, No. 5 (2016) pp.107-118.