ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review on Watermarking Techniques for Biometrics

Amanpreet Kaur Wadhwa
Department of Computer Science
Guru Kashi University
Bathinda, India

Monica Goyal
Department of Computer Science
Guru Kashi University
Bathinda, India

Abstract: Watermarks are used for decades to verify and authenticate RGB images. Now days, watermarks are incorporated into digital graphics so that original owners can keep their right and ensure the originality of the digital data. However, the biometric images such as fingerprints, are being transferred over internet daily or in a remote AFAS system where database is on other location, thus increasing risk of attacks during transmission. Receivers need a verification system which can verify the integrity of the content. If the images are watermarked, it is easy for the owner to check and verify the images. Every day, lots of development and improvement is being conducted in different branches of this stream. Steganography is used for secure communication, whereas watermarking is used for image and content protection, copyright saving, content authentication and tamper detecting in this paper we present a thorough survey of current existing and newly developing steganography and watermarking techniques.

Keywords: Watermarking, Watermark Detection, Spatial Domain, Image Transforms, DWT, DCT, DFT.

I. INTRODUCTION

Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. [13] The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents [13]. In order to protect the interest of the content providers, these digital contents can be watermarked. In this paper, we provide a survey of the latest techniques that are employed to watermark images.

A general method for establishing the identity of a person is essential in all transactions whether they are commercial or non-commercial. The ability to establish identity with certainty can prevent forgery and fakes [1]. In year 1980, this remains a major concern in electronics, e-commerce, telecommunications, biomedical, and security. While verifying the identity of individuals it was primarily handled with information such as a passport number, adhaar card number or a password, or a photo ID [12]. However, these methods are gradually losing security and speed thereby getting replaced by biometrics, such as fingerprint, gait, speech and iris, which are "unique" to an individual and so they cannot be easily altered [1].

Watermarks are best used for authentication and to prevent fraud. Most expensive products have an embedded logo, like currency. These watermarking schemes are easy and serve their purpose efficiently in every manner. Reproducing watermarked notes is impossible. Considering their success to date, applying (digital) watermarks to biometric data and identifiers is a better approach to determine their ownership and avoid tampering [2]. Now days, visible watermarks are outdated and invisible watermarks are in vogue. Invisible watermarks, as their name indicates are not visible and negligibly affect the data that they are embedded in. This method is desired if one does not want to perceptually change the image quality.

II. REQUIREMENTS OF DIGITAL WATERMARKING

There are three main requirements of digital watermarking technique which are transparency, robustness, and stability of tampering and can be effectively used.

A. *Transparency or Fidelity*

The digital watermark should not affect the quality of the original image after it is watermarked [3]. Cox et al. define transparency or fidelity as "perceptual similarity between the original and the watermarked versions of the cover work" [7].

Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the commercial value of the image [7].

B. *Robustness*

Cox et al. defines robustness as the "ability to detect the watermark after common signal processing operations" [7]. Watermarks could be removed intentionally or unintentionally by simple image processing operations like contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against variety of such attacks. Stirmark[2] classifies attacks into four basic categories, attacks that try to remove watermarks totally, attacks that try to remove the synchronization between the embedded and the detector, crypto graphic attacks and protocol attacks.

C. *Capacity or Data Payload*

Cox et al. define capacity or data payload as "the number of bits a watermark encodes within a unit of time or work" [7]. This property describes how much data should be embedded as a watermark to successfully detect during extraction. Watermark should be able to carry enough information to

represent the uniqueness of the image. Different application has different payload requirements [1].

III. WATERMARKING APPLICATIONS

Before beginning the discussion on watermarking algorithms we discuss the applications. The main applications of digital watermarking are discussed here.

A. Copyright Protection

Watermarking can be used to protecting redistribution of copyrighted material over the non trusted network like Internet or peer-to-peer (P2P) networks. Content aware networks (p2p) could incorporate watermarking technologies to report or filter out copyrighted material from such networks.

B. Content Archiving

Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a very fragile technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the pos-2 Stir mark is a benchmark to test robustness of watermarking algorithms.

C. Meta-data Insertion

Meta-data refers to the data that describes data. Images can be labeled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records [10].

D. Broadcast Monitoring

Broadcast Monitoring refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on TV or Radio) has really been broadcasted or not. Watermarking canal so be used for broadcast monitoring. This has major application in commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration.

E. Tamper Detection

Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicated the presence of tampering and hence the digital content cannot be trusted [8]. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not [9].

F. Digital Fingerprinting

Digital Fingerprinting is a technique used to detect the owner of the digital content. Fingerprints are unique to the owner of the digital content [5]. Hence a single digital object can have different fingerprints because they belong to different users.

IV. WATERMARKING TECHNIQUES

Many different watermarking schemes have been developed till now. One of the first watermarking techniques involved altering the least significant bit (LSB) of pixels in the spatial domain [6]. There are many different ways in which these LSB schemes can be applied. For example, either all the LSBs could be changed, or a randomly chosen set of LSBs could be changed [12]. If one alters an image, it is more than likely that the LSB will be altered as well. Unfortunately, this same fragileness can cause a host of other problems. It makes it possible to obliterate the whole watermark. If a sufficient number of LSBs are changed, the watermark becomes unrecoverable [6].

On the other hand, it is also possible to alter an image without changing the Least Significant Bits. If this is done, the watermark does not remain with any purpose, as it cannot be used to identify tampering. In general, pixel level domain techniques are too fragile to bear an attack. Thus, frequency domain techniques have been developed. Generally there are two frequency domain algorithms, a spread spectrum method and a block method [7].

The DCT of the complete image is done, and the watermark is applied to pre-selected frequencies. For example, if the image DCT is represented by I (j, k), and the watermark is W (j, k), then the watermarked image is $W^*(j, k) = I (j, k) + \alpha W (j, k)$, where W (j, k) has the normal distribution and α is a scaling parameter. In the simple version of the method, the value of alpha is set to 0.1. For more good results, α can be derived from just noticeable difference matrix [12]. The JND matrix has the average value that can be incremented to each pixel without causing a change in the image pixels [12]. It is very similar to the spread spectrum technique, however instead of taking the DCT of the complete image, the DCT is taken for 8x8 (or 16x16, etc.) blocks [6].

In this way, localization of watermarks is done having the advantage since it is compatible with lossy type of the compression techniques like JPEG. It could be built straight into a JPEG processor. As it is applied to each image segment separately, it is simpler to remove this type of a watermark [8].

With the popularity of the JPEG format, developing watermarks that could be compressed are very difficult. In these techniques the watermark is often inserted into the frequency domain of the compressed original image. When watermarks are hidden into uncompressed images, the watermark gets damaged after compression [5]. In fact, it can be damaged and is no longer recognizable. But by inserting the watermark in the compressed frequency domain, compression have very little effect on the watermark (when culprit does not compress the image to a level much below where the watermark was placed) [9]. Another embedding scheme that is usually discussed involves placing multiple watermarks into a single image. By placing more than one watermarks into the single image, the ability to determine whether an image has been altered/tampered with and where it has been tampered with increases.

General, two watermarks are placed into a single cover image, out of which one of the watermarks is robust to image processing and the other detects minor alteration in the

images. In various studies, a watermark was inserted into the frequency domain (robust watermark) as well as into the pixel domain (fragile watermark) [10]. There are a couple of drawbacks to this type of techniques.

Also when embedding the watermarks it is essential to insert the robust watermark first [11]. If the fragile watermark is inserted first, then as soon as robust watermark is embedded, the fragile watermark will identify non-existent tampering.

V. DCT DOMAIN WATERMARKING

DCT based watermarking techniques are more robust compared to simple spatial domain watermarking techniques [5]. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring, etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping, etc.

DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. One of the first algorithms presented by Cox et al. used global DCT approach to embed a robust watermarking the perceptually significant portion of the Human Visual System (HVS) [7]. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image. In spatial domain it represents the LSB however in the frequency domain it represents the high frequency components [3].

VI. DWT DOMAIN WATERMARKING

In the last few years wavelet transform has been widely studied in signal processing in general and image compression in particular. In some applications wavelet based watermarking schemes out performs DCT based approaches.

One such scheme is proposed here [4]. Hence it makes it an important to pick for research.

A. Characteristics of DWT

1. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect an isotropic properties of HVS more precisely [4] [1].

2. Wavelet Transform is computationally efficient and can be implemented by using simple filter convolution.

3. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL) [4] [2].
4. The larger the magnitude of the wavelet coefficient the more significant it is.
5. Watermark detection at lower resolutions is computationally effective because at every successive resolution level there are few frequency bands involved.

6. High resolution sub bands helps to easily locate edge and textures patterns in an image.

VII. CONCLUSION

Watermarking of the biometric such as fingerprint, iris, etc. is a still a relatively new idea, but it is of increasing importance as more robust methods of verification and authentication are being used. Biometrics provide high security but their validity must be integral which can be increased by watermarks. Unfortunately, they cannot provide a fool proof solution especially when the transmission of data is involved. A receiver cannot always determine if he/she has received the correct data without the sender giving her access to code or password (i.e., the watermark). Thus data security can be assured in databases as well as in transmission over internet.

VIII. REFERENCES

[1] A. K. Jain, L. Hong and S. Pankanti. "Biometric Identification", Comm. ACM, vol. 43, no. 2, pp.91-98, Feb. 2000.

[2] S. Pankanti and M.Y. Yeung, "VerificationWatermarks on Fingerprint Recognition andRetrieval", in Proceedings of the SPIE/IS&TElectronic Imaging '99.

[3] V.S. Nalwa. "Automatic On-line Signature Verification", in Proceedings of the IEEE, vol.85, pp.215-239, Feb.1997.

[4] M. Wu, E. Tang and B. Liu. "Data Hiding in aBinary Image". To appear in ICIP '00 .

[5] M. Riezenman. "Cellular Security: better, butfoes still lurk", in IEEE Spectrum, vol. 37, pp.39-42, 2000.

[6] R.G. van Schyndel, A.Z. Tirkel, and C.F.Osborne. "A Digital Watermark", in Proceedingsof the IEEE International Conference on Image Processing, vol.II, pp. 86-90, 1994.

[7] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon."Watermarking for Multimedia", NEC Research Institute Technical Report, 95-10, 1995.

[8] C. Hsu and J. Wu. "Hidden Signatures inImages". IEEE ICIP III '96, pp. 223-26.

[9] M. Wu, H. Yu, A. Gelman. "Multi-level DataHiding for Digital Image and Video", SPIEPhotonics East '99, Boston 1999.

[10] J. Fridrich, "A Hybrid Watermark for Tamper Detection in Digital Images", ISSPA '99. pp.301-304.

[11] F. Minzer and G.W. Braudaway. "If OneWatermark is Good, are More Better?", IEEE'99, pp. 2067 -2069.

[12] Jain, Sonia. "Digital watermarking techniques: a case study in fingerprints & faces." *Proc. Indian Conf. Computer Vision, Graphics, and Image Processing*. 2000.

[13] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." *Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on*. IEEE, 2005.