Review of digital watermarking mechanisms

Rohit Kumar[1], Sorab kumar[2]

M.tech Research schollar[1], Assistant professor Department of CSE-SSCET Badhani[2]

Abstract:

Now days the protection and illegal redistribution of digital media has become a major issue. The digital watermarking has been used to protect digital information from illegal redistribution and changes. In digital water marking the image has been enhanced by embedding noise tolerant signal into carrier signal. The study of various technique of digital watermarking has been done in this paper; also the contribution of watermarking techniques for security purposes has been analyzed.

Keywords: digital watermarking, noise tolerant, carrier signals, security

INTRODUCTION

Watermarking can be measured as unique strategies of steganography where one message is embedded in another and the two messages are identified with each other. Computerized watermarking is like watermarking procedure which enables a person to include select rights notices or other confirmation messages to advanced media. Picture verification's one of the uses of advanced watermarking, which is utilized for authenticating the computerized pictures. An advanced watermark is a sort of marker secretively installed in a noise tolerant picture, for example, sound or picture information. It is regularly used to recognize responsibility for copyright of such picture. "Watermarking" is the way toward hiding away computerized data in a picture the hidden data ought to yet do not have to contain a relation to the picture. The major issue now days are security of academics information. The best approach to understand this element is to embed a level of the verification signature into the advanced picture utilizing a computerized watermark. On account of the picture being altered, it can without much of a stretch been identified as the pixel estimations of the embedded information would change and don't coordinate with the first pixel esteems. There are numerous spatial and recurrence space procedures are accessible for validation of watermarking. Watermarking procedures are judged on the premise of their execution on a little arrangement of properties. Watermarking plans are produced by the prerequisites of the application and all applications don't require each of these properties completely i.e. watermarking necessities are application reliant and some most desirable properties for these applications are clashing in nature.

Be that as it may, [1]if the watermarking strategy isn't related to the security purposes at that point open watermarks are used and the watermarked image is easily gotten to by anyone. The whole watermarking technique should take after two phases: introducing and removing. In the embedding technique, the watermark media is introduced or inserted into the primary image. Resulting to embedding's, a watermarked image is obtained. In the expelled methodology, the watermark is isolated from the watermarked image by following an inverse of embedding strategy. That expelled watermark is required at the recipient level for gaining the supportive information (watermark). Watermarking is done by following a particular system. The idea of the watermarked image is extremely depends on the watermarking strategy used. Spatial Domain methodologies are used for performing watermarking. The watermarking is done by changing the scarcest immense bits of the image in by far most of the spatial area frameworks. In any case, these frameworks are not healthy and unclear. So to get incredible nature of watermarked image, recurrence area strategies are used. In recurrence space frameworks, coefficients estimations of the image are changed by following a particular recurrence area system. The recurrence space techniques are more intense and unpretentious than the spatial area frameworks. The idea of the watermarked image of the recurrence space procedures is incredibly enhanced than the idea of the watermarked image procured by spatial area strategies.

Techniques used for Image security

To achieve the image security, watermarking and steganography mechanisms commonly followed. The techniques for image security are described as under

LSB Steganography

[2]In LSB steganography, the least significant bits of the image are chosen and replaced with the logo image. The contrast enhancement mechanism is implied in order to change the contrast of both the images so that merged images are clearly visible.

Problem with this approach is however that attackers easily can determine the position of the logo and hence attack can easily takes place. In order to tackle the issue, MSB steganography is followed.

MSB Steganography

[3]In MSB steganography, most significant bits are enriched with the logo image and hence merged image is obtained. The assumption is that MSB are less prone to attacks as compared to LSB bits. The mechanism of LSB steganography is performed in this case however MSBs are used in place of LSBs.

Cipher Bits

[4]This is another mechanism to ensure the safeguard of transmitted image over the career. The image meant to be transmitted over the medium however before transmission image is encoded and cipher image is obtained. The key that can be public or private is also generated. This key is transmitted along with the image itself. At the other end decryption mechanism is implied to resolve the problem into desired image formats.

AES

[5]Advanced encryption slandered can be used in order to provide encryption of images for security. AES provide 128 bit encryption with 32 distinct segment formats. Keys are generated which are shared with sender and receiver. Keys are used to decode the image which is received at the destination end.

Image Authentication

[6]This is the mechanism in which username and password is allocated to the image. In order to access the image username and password is required to be given. The wrong password ensures de-allocation of resources. Image authentication is least secure since passwords can be easily guessed. In order to overcome this situation, image watermarking mechanism can be used.

Next section describes the literature survey if existing mechanism used for image security.

Literature Survey

The techniques associated with image encryption are described in this section. [7] Proposed field of signal processing the technology of image watermark is very important. In this paper the knowledge of image watermark' as well as the DCT/IDCT had been introduced. Encryption algorithm had been introduced in which the watermarking information was based on the size of the image. To verify this watermarking algorithm by MATLAB the watermark's embedding and extraction had been performed on two images. The result shows that the adaptive algorithm is very effective. [8] Proposed technology is improving in a great way with this improvement in imaging skill. The ease with which digital content can be imitated and operated there is a strong requirement for a digital patent device to be put in place. It is required for the authentication of the content as well as the owner and digital watermarking is the solution to resolve this problem. We have several watermarking techniques have been introduced now. In this paper we survey the current schemes that have been developed with their effectiveness.

In [9] paper High efficiency video coding (HEVC) is the new video coding generation of the ITU-T and ISO/IEC, which was first appeared in January 2013. Its main advantage is that it reduces the bit rate by as much as 50 % when compared to H.264 even though visual quality is maintained. In order to protect video contents by embedding within an efficient video codec authentication and copyright protection methodologies have become one of the essential items. The main objective of this paper is to revise recent developments in the area of watermarking techniques for video coding schemes and their applicability to the new Standard HEVC.

[10] Proposed paper works on medical information digitization storage and extraction process more convenient. In Medical image information the security and copyright protection is taken so seriously, so that medical image watermarking has been applied. This paper proposes a robust zero-watermarking algorithm.

[11] Proposed paper presents digital images watermarking to provide ownership and true authentication. To secure the images, audio and videos, Firstly watermark W is converted into a sequence of bits and in order to encrypt the watermark, sequence of size R is selected randomly. Secondly, a pseudo random number is generated to calculate pixels for selection key generation. Finally, 2-level discrete slanted transform (DST) on the host image is applied to divide it into Red, Green and Blue channels. The

results exhibit robustness against the existing state of the art. Further, In the absence of the original images proposed approach effectively extract watermark.

[1] Proposed paper uses watermarking scheme in which a mark is dropped into a program while preserving its functionality. Nobody can remove the mark without damaging the functionality of the program. In this paper various problems of watermarking cryptographic programs such as pseudorandom function (PRF) evaluation, decryption, and signing are studied.

In [12] proposed paper for copyright protection of multimedia data, Digital watermarking is one of the best solution. It is better than Digital Signatures and other methods because it does not increase overhead. To hide information, for example a number or text, in digital media, such as images, video or audio digital watermarking is used.

[13] Proposed paper discussed Digital watermarking for the improvement and robustness in multimedia. This paper presents an overview of secure watermarking technique. For each context, a threat analysis is purposed. This study allows us to illustrate all the certainties the community has on the subject, browsing all key papers. In future vague facts, intuitions will be discussed.

COMPARISON OF VARIOUS IMAGE WATERMARKING TECHNQIUES

TITLE AND REFERENCE	JOURNAL/CONFERENCE	TECHNIQUE	MERIT	DEMERIT
[11] Digital Watermarking for Images Security using Discrete Slantlet Transform	NSP	DST	Effective extraction of features for security enhancement	Complex due to heavy mathematical calculations
[14] Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain	IJCA	Spatial Domain based on LSB- Based, Statistical-Based, Feature-Based and Block-Based	Analysis of various techniques for security enhancement is presented which can be used for further enhancement in image security	No parameter wise description is presented
[15] A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform	IEEE Conference	DCT	Application of DCT is presented for enhancement of security in terms of data hiding in images	Time complexity of overall operation is high due to limited modularity
[5] An Integration of SVD Digital Image Watermarking with AES Technique for Copyright Protection and Security of Bank Cheque Image	IEEE	SVD	Singular valued decomposition provides least complexity in terms of gray scale images hence classification is better	Coloured images cannot be tackled
[7] Research on Image	SCIENCE DIRECT	DCT	Watermarking	Complexity in

Watermarking Algorithm based on DCT			security is enhanced using DCT	terms of space and time is high
[16] Protecting Digital Images Using DTCWT-DCT	IEEE	DTCWT-DCT	Hybridization is done to reduce time complexity. Image watermarking security is enhanced using proposed technique	Space complexity is high and nothing is suggested to reduce this complexity
[17] Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method	IEEE	DCT AND DWT	Modularity is enhanced due to the application of DWT	Complexity of mathematical calculations is high due to DCT
[18] Biometric Template Security based on Watermarking	SCIENCE DIRECT	BIOMETRIC SECURITY	Biometric security is enhanced through watermarking	Hybridization of multiple approaches is missing
[2] An Improved Image Steganography Technique based on MSB using Bit Differencing	IEEE	IMAGE STEGNOGRAPHY	MSB Stegnography is used for image security	MSB Stegnography may lead to distortion within the image
[19] New Proposed Practice for Secure Image Combing Cryptography Steganography and Watermarking based on Various Parameters	IEEE	CRYPTOGRAPHY, STEGNOGRAPHY AND WATERMARKING	Enhanced security is achieved through the application of hybridization	Complexity of operation is enhanced

Table 1: Comparison of Image Encryption Techniques

CONCLUSION

The security within transfer of information is critical. Various techniques such as encryption, steganography etc. has been evolved over the years the efficiency and energy consumption associated with these techniques still require improvement .Watermarking security is one of the alternatives for enhancing the security process. The watermarking security utilizes two consecutive images and merges them together, after merging images transferred towards the destination. In case of corruption images distorted and techniques such as SVD, DWT can be used to analysis such images. MSE and accuracy associated with SVD, DWT is not optimum.

So in future slant let transformation along with SVD can be used in order to improve MSE and accuracy.

REFERENCES

[1] A. Cohen, "Watermarking Cryptographic Capabilities ∗."

[2] A. U. Islam *et al.*, "An improved image steganography technique based on MSB using bit differencing," *2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016*, pp. 265–269, 2017.

[3] V. Saravanan and A. Neeraja, "Security issues in computer networks and stegnography," *7th Int. Conf. Intell. Syst. Control. ISCO 2013*, pp. 363–366, 2013.

[4] P. Singhai and A. Shrivastava, "An efficient Image Security mechanism based on Advanced Encryption Standard," no. 13, 2015.

[5] S. S. Gonge, "An Integration of SVD Digital Image Watermarking with AES Technique for Copyright Protection and Security of Bank Cheque Image," pp. 769–778, 2016.

[6] Q. Chen, H. Hu, and J. Xu, "Authenticated Online Data Integration Services," pp. 167–181.

[7] Z. J. Xu, Z. Z. Wang, and Q. Lu, "Research on Image Watermarking Algorithm based on DCT," vol. 10, pp. 1129–1135, 2011.

[8] G. Tiwari, "A Review on Robust Watermarking with its Applications and Comparative Analysis," vol. 8, no. 6, pp. 85–90, 2015.

[9] U. Tun and H. Onn, "RECENT METHODS AND TECHNIQUES IN VIDEO WATERMARKING AND THEIR APPLICABILITY TO THE," vol. 74, no. 1, 2015.

[10] B. Han, L. Cai, and W. Li, "Zero-watermarking Algorithm for Medical Volume Data Based on Legendre Chaotic Neural Network and Perceptual Hashing," vol. 8, no. 1, pp. 201–212, 2015.

[11] M. Mundher, D. Muhamad, A. Rehman, T. Saba, and F. Kausar, "Digital Watermarking for Images Security using Discrete Slantlet Transform," vol. 2830, no. 6, pp. 2823–2830, 2014.

[12] P. Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data," vol. 3, no. 9, pp. 1–4, 2012.

[13] T. Furon, "A Survey of Watermarking Security," pp. 201–215, 2005.

[14] R. V Mahule, "Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain," no. Nckite, pp. 19–26, 2015.

[15] I. Science and W. No, "A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform Yang Qianli," pp. 1102–1105.

[16] K. Ramani, E. V Prasad, and S. Varadarajan, "Protecting Digital Images Using DTCWT-DCT," pp. 36–44.

[17] R. K. Sheth and V. V. Nath, "Secured digital image watermarking with discrete cosine transform and discrete wavelet transform method," *2016 Int. Conf. Adv. Comput. Commun. Autom.*, pp. 1–5, 2016.

[18] G. Bhatnagar, Q. M. J. Wu, and B. Raman, "Biometric Template Security based on Watermarking," *Procedia Comput. Sci.*, vol. 2, pp. 227–235, 2010.

[19] R. Gupta and T. P. Singh, "New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters," *Proc. 2014 Int. Conf. Contemp. Comput. Informatics, IC3I 2014*, pp. 475–479, 2014.