www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13553-13558

Text Watermarking Approaches for Copyright Protection

Gagandeep kaur, Sukhwinderbir
Student: Department of C.S.E
Beant College of Engineering and Technology
Gurdaspur,India
gagan2740@yahoo.co.in
A.P:Department of C.S.E
Beant College of Engineering and Technology
Gurdaspur,India
sukhwinderbir@gmail.com

ABSTRACT : ***With far reaching utilization of Internet and other correspondence advances, it has ended up to a great degree simple to imitate, impart, and appropriate computerized substance. Accordingly, validation and copyright insurance issues have emerged. Content is the most widely utilized medium going over the Internet other than picture, sound, and feature. The real piece of books, daily papers, website pages, promotion, exploration papers, authoritative reports, letters, books, verse, and numerous different records is essentially the plain content. Copyright insurance of plain content is a huge issue which can't be approved. The current answer for watermarking of plain content archives are not powerful towards irregular altering assaults and are inapplicable for various spaces. In this paper, we have clarified content watermarking and its different systems.***

KEYWORDS: WATERMARKING, AES, DES, PROTECTION.

INTRODUCTION

In today's reality web get to be massive territory for imparting information, getting to data, transmission of information starting with one piece of the world then onto the next [1]. On the web diverse kind of information is accessible like content, picture, sound, feature etc. Presently a day's much instructive association, saving money parts, businesses utilizes web for their working and exchanges. So they need to shield the information from outside world for unlawful getting to of data. Shield information from illicit powers there are different technique in computerized world like cryptography, steganography, watermarking. In steganography primary idea is encryption and decoding of information. If there should arise an occurrence of encryption information is scrambled and outside world or outsiders can't get to it. At that point on collector side in the wake of unscrambling there is no any procurement to shield information from replications. With the goal that there is some other method is required so as to demonstrate and give the responsibility for, dodge illicit access to that information, shield it from adapting and give certain kind of confirmations [2]. The system came as a main priority in the wake of concentrating on above issues is that advanced watermarking. The fundamental thought of computerized watermarking is to insert advanced data into advanced information such that it can't be effortlessly distinguished and evacuated. The computerized data and in addition advanced information possibly content, picture, sound, feature or mix of anything [3].

WATERMARKING

Watermarking is a branch of data concealing which is utilized to cover up extra data in computerized media like picture, sound, feature, or content. Computerized watermarking strategy alludes to the procedure of installing the given watermark data, (for example, possession data, name, logo, signature, and so on.) in the defensive data, (for example, picture, sound, feature, or content) and picking the given watermark data from the defensive data, which in not saw by human perceptual framework [4].

As it were, watermarking is a procedure of inserting a computerized sign or watermark containing data remarkable to the copyright proprietor in the article (content, picture, sound, or feature) which is expected to be ensured. An advanced watermark is characterized as an unmistakable or undetectable ID code that is for all time inserted in the information, to transmit concealed information. It stays introduce in the information even after the decoding methodology. It more often than not gives copyright insurance of licensed innovation [5]. The watermark is later used to recognize the accepted copyright proprietor of the article.

WHY TEXT WATERMARKING IS DIFFICULT?

Plain content, being the easiest method of data, conveys different difficulties in the matter of copyright assurance. Content has constrained limit for watermark installing since there is no excess in content as can be found in pictures, sound, and features. The paired nature with clear division in the middle of closer view and foundation, piece/line/word designing, semantics, structure, style, and dialect tenets are a portion of the famous properties of content which are expected to be tended to in any content watermarking calculation [6]. Furthermore, the inalienable properties of a nonexclusive watermarking plan like indistinctness, strength, and security additionally need to be fulfilled. Any change on content ought to save the significance, familiarity, grammaticality, and the estimation of content. The importance of the content is its esteem, and it ought to be protected through watermarking in place not to irritate the correspondence. Familiarity is obliged to speak to the importance of the content in an unmistakable and familiar way, all the more vitally in artistic compositions. The inserting procedure ought to consent to the punctuation principles of the dialect, keeping in mind the end goal to protect the clarity of the content. Protecting the style of the writer is essential in a few areas, for example, writing composition or news channels [7]. Delicate nature of a few reports, for example, authoritative records, verse, and quotes don't permit us to make semantic changes haphazardly on the grounds that in these types of content a basic change now and again decimates both the semantic intention and the estimation of content.

Watermarking Processes

The procedure of watermarking includes 4 stages [8].

1. Watermark Generation

2. Watermark Insertion

3. Watermark Detection

4. Watermark Extraction

1. Watermark Generation: In this procedure there are two conceivable outcomes one is guide some special advanced flag as watermark is embedded and another is extraordinary watermark is created utilizing certain method.

2. Watermark Insertion: As watermark is created it is embedded in unique advanced flag by some insertion process at certain position.

3. Watermark Detection: In this methodology client over the web, outsiders, unlawful powers, assailant and so on simply recognize or identify that computerized archive contains watermark or not.

4. Watermark Extraction: This procedure is performed at beneficiary side it extricate watermark from computerized record by utilizing opposite methodology of embedding's watermark [9].

TEXT WATERMARKING ALGORITHM

The text watermarking calculation comprises of four sections: the watermark, the encoder (insertion calculation), the finder and the comparator (confirmation or extraction or location calculation) [10].

It expect a unique content record O, a mystery key K=k1, k2,… ki, watermark M and the watermarked content report W. Watermark M is inserted after the key. The insertion capacity E produces a watermarked content record T' compare to the info of O, M and K. The capacity E is spoken to by

E (O, K, M) = W [1]

The identifier capacity D takes a content record (H is an associated unlawful content archive with O. H is at any rate looks like O) and copyright proprietor's key K=k1, k2,… ki then it extricate watermark M'. The capacity D is spoken to by

D (H, K) =M' [2]

A look at capacity C takes M' as an info to contrast and all M recorded in its framework information base.

C (M', M) = 1; if M'=M, generally C (K', K) =0 if M'≠M.

The accompanying figure outlines over three capacities and the entire content watermarking calculation. Accept it is in the advanced library situation.

TECHNIQUES USED FOR TEXT WATERMARKING

There are various technique that are used for watermarking but two of them are given as:

a) **AES** - It is a web instrument to scramble and decode content utilizing AES encryption calculation. You can picked 128, 192 or 256-bit long key size for encryption and unscrambling. The consequence of the procedure is downloadable in a content record. AES (acronym of Advanced Encryption Standard) is a symmetric encryption calculation. The calculation was produced by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was intended to be proficient in both equipment and programming, and backings a square length of 128 bits and key lengths of 128, 192, and 256 bits [11].

b) **DES**- The Data Encryption Standard is a piece figure, importance a cryptographic key and calculation are connected to a square of information all the while instead of one bit at once. To encode a plaintext message, DES bunches it into 64-bit squares. Every square is enciphered utilizing the mystery key into a 64-bit figure message by method for stage and substitution. The procedure includes 16 rounds and can run in four distinct modes, scrambling squares separately or making every figure piece subject to all the past pieces. Unscrambling is essentially the reverse of encryption, taking after the same steps yet turning around the request in which the keys are connected. For any figure, the most

essential strategy for assault is animal power, which includes attempting every key until you locate the right one. The length of the key decides the quantity of conceivable keys - and thus the plausibility - of this kind of assault. DES utilizes a 64-bit key, however eight of those bits are utilized for equality checks, adequately restricting the way to 56-bits. Thus, it would take a most extreme of 2^56, or 72,057,594,037,927,936, endeavors to locate the right key [12].

S.no.	Author Name	Technique Used	Algorithm Used	Result
1.	Prabhjot Kaur Cheema and Kamaljit Kaur	In the proposedtechnique components of English language like noun, pronoun, model verbs and conjunctions of user's choice alongwith author id are used to create watermark of user's choice. Moreover, encryption techniques AESalgorithm is applied to encrypt watermark and to enhance its security level to protect it from tamperingattacks and to prove the most robust algorithm	AES	67%(Accuracy)
2.	BidyutJyotiSaha,Kunal Kumar Kabi,Arun and Chittaranjan Pradhan	In this paper, we have proposed a robust watermarking algorithm using DES, ECC and DCT for color images. The original color image (watermark) and cover image has been separated into three independent color channels (red, green and blue) and their gray scale equivalents are used. Each individual gray scale equivalent of RGB components of original image has been encrypted using Data Encryption Standard (DES). The Henon map is used to generate three different	DES	51-55% (PNSR)

		round keys for DES with different initial parameters.		

CONCLUSION

This paper incorporates the idea of advanced watermarking and content watermarking. It gives basic data of diverse systems for content report watermarking. Audit on different methods which are similar to Advanced Encryption Standard and Data Encryption Standard. This paper likewise incorporates the different proposed methods which can enhance the watermarking strategies for more security, heartiness, carefully designed executionand so on.

REFERENCES

[1] ZuneraJalil and Anwar M. Mirza, "A Review of Digital Watermarking Techniques for Text Documents", IEEE International Conference on Information and Multimedia Technology, pp. 230-234, 2009.

[2] Yanqun Zhang, "Digital Watermarking Technology: A Review", IEEE International Conference on Future Computer and Communication, 2009.

[3] L.Robert and T. Shanmugapriya, "A Study On Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, Vol.1, No. 2, pp. 223-225, May 2009.

[4] M. Topkara, G. Riccardi, D. Hakkani-Tur, and M. J. Atallah, "Natural language watermarking: Challenges in building a practical system", *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents*, San Jose, CA, Jan. 2006.

[5] A. Khan, A. M. Mirza, and A. Majid, Optimizing Perceptual Shaping of a Digital Watermark using Genetic Programming, Iranian Journal of Electrical and Computer Engineering, vol. 3, no. 2, pp. 144-150, 2004.

[6] A. Khan and Anwar M. Mirza, Genetic Perceptual Shaping: Utilizing Cover Image and Conceivable Attack Information Using Genetic Programming, Information Fusion, vol. 8, no. 4, pp. 354-365, 2007.

[7] A. Khan, Intelligent Perceptual Shaping of a digital Watermark, PhD Thesis, Faculty of Computer Science and Engineering, GIK Institute, Pakistan, 2006.

[8] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O. Gorman, Electronic Marking and Identification Techniques to Discourage Document Copying, IEEE Journal on Selected Areas in Communications, vol. 13, no. 8, pp. 1495-1504, 1995.

[9] J. T. Brassil, S. Low, N. F. Maxemchuk, L. O. Gorman, "Hiding information in document images", in Proceedings of the 29th Annual Conference on Information Sciences and Systems, Johns Hopkins University, 1995, pp 482-489.

[10] Huijuan Yang, Alex, and C. Kot, "Text Document Authentication by Integrating Inter Character and Word Spaces Watermarking", IEEE Inter-national Conference on Multimedia and Expo. , Vol.2, pp. 955 –958, June 26-30, 2004.

[11] Zhichao Yu and Xiaojunliu, "A New Digital Watermarking Scheme Based on Text", IEEE Inter-national Conference on Multimedia

Information Networking and Security, Vol. 2, pp. 138-140, 2004.

[12] Nighat Mir and Sayed Afaq Hussain, "Web Page Watermarking: XML files using Synonyms and Acronyms", World Academy of Science, Engineering and Technology, Issue 49, Jan 2011.