Review of Copyright Protection for Digital Image Watermarking using Encryption Process

Shubham Kushwaha[1*], Aman Sharma[2*]

[1]M. Tech. Scholar, Department of Electronics and Communication Engineering, Samrat Ashok Technological Institute, Vidisha, M.P. India,

[2]Assistant Professor, Department of Electronics and Communication Engineering, Samrat Ashok Technological Institute, Vidisha, M.P. India,

Abstract: - The development of the computerized period has changed the data procurement, stockpiling and transmission to the advanced structure. The digitalization of data has made its procurement, stockpiling and transmission forms to be help. The simplicity of these procedures has expanded the utilization of computerized data by more extensive scope of individuals. Likewise, the simple access to this data makes it unreliable to be put away and transmitted with no veil. The transmission of the advanced data normally happens in the open system where it tends to be altered or caught by meddlers. Past the security issues, the advanced period additionally faces a test in dealing with the hole that emerge between the measure of advanced data that is being created and the ability of putting away and handling the data created.

As an exertion of improving the security by making the encryption process plain picture dependent just as unique in nature, the second calculation changes the disarray procedure. The plain picture disarray is finished by permuting the pixel esteems utilizing two picture dependent frameworks and with an extra powerful substitution. These procedures increment the affectability of the encryption plan to the plain picture just as key. The plain picture affectability can expand the obstruction of the plan against differential assaults.

Keywords: DWT, DCT, PSNR, NC

I. INTRODUCTION

The quick advancement of computerized interactive media innovations, fast web and modest accessibility of multi-media records tremendously affected advanced media verification. These days, the transmission of interactive media information got normal everyday practice. Assurance of the scholarly copyrights of interactive media content is testing issue because of illicit duplicating and conveyance. Advanced watermarking is successful and famous answering for address this issue [1]. For the most part watermarking is worked on mixed media content like picture, video, content and sound. Computerized watermarking embeds the watermark information into sight and sound substance to show proprietorship and credibility. Advanced watermarking has a few applications like copyright security, duplicate insurance, sealing, communicate checking, fingerprinting, get to control, restorative applications, etc. Computerized watermarking process includes two stages viz., Embedding and Extraction [2].

The general watermarking process is appeared in Figure 1. The watermark embedder comprises of two sources of info, the first substance (sound or picture or video or content) called as host sign and information which is inserted is called as watermark. Embedder embeds watermark in the host and produce watermarked signal. Hiding process is so controlled with the end goal that the implanted watermark ought not corrupt host sign or watermark can't be expelled by different assaults. This watermarked content is presently accessible to open. Any individual/outsider may make a change to this substance so as to alter or expel the watermark. Watermark extractor endeavors to acquire watermark from the watermarked signal [3, 4]. Dependable extraction is conceivable when watermark isn't influenced by SP and DS assaults. Consequently, a hearty extraction process is required to get watermark precisely by beating these assaults.

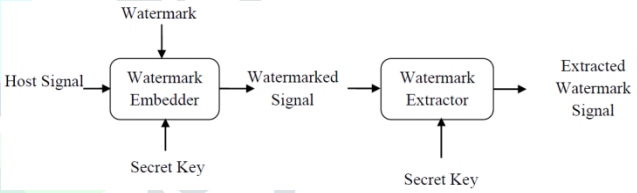

Fig. 1: Embedding and Extraction Process of Watermark

In view of the kind of advanced sight and sound as host, watermarking methods can be arranged into four classifications is appeared in Figure 2.

- Text Watermarking – It is a procedure to install a watermark into a book record.
- Image Watermarking – It is a procedure to insert either picture, or sound, or content as watermark into a computerized picture.
- Video Watermarking – This procedure inserts a watermark (any interactive media) into have advanced video.
- Audio Watermarking – In this, computerized sound is treated as spread sign and picture or sound goes about as watermark.

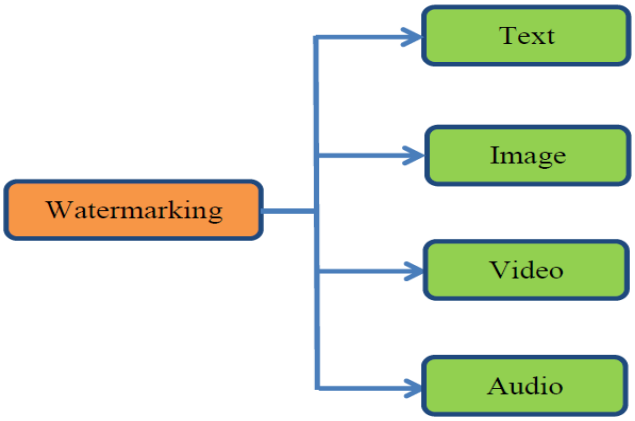

Figure 2: Types of Watermarking

II. LITERATURE REVIEW

Watermarking goes back to 1990s and began taking part in computerized upset (Ingemar J COx, Matthew L Miller, Jeffrey A Bloom, Jessicah Fridrich 2008). Later on, there has been a critical spotlight on computerized portrayal of sound. Advanced Audio Watermarking (DAW) is a procedure of concealing sight and sound substance. It involves covering of watermark in have sound; to get watermark when basic to give copyright insurance, confirmation and Digital Rights Management (DRM) purposes. First precise exertion on DAW was accounted for in 1997 (Cox et al., 1997). Later on, numerous scientists concocted diverse DAW plans and a noteworthy work has been accounted for on DAW over the most recent two decades.

The viability of a DAW conspire is portrayed by different execution criteria (A.Spanias and T.Painter 2007) viz., strength, subtlety, payload, security, computational multifaceted nature, and so forth. Power is the capacity of solid watermark extraction despite the fact that watermarked sound is influenced by assaults. Impalpability alludes to the nature of the sound sign subsequent to implanting the watermark. The expansion of watermark acquaints little modifications with the host which are perceptually unclear. Thus, impalpability is additionally named as straightforwardness, loyalty and unintelligibility. Payload is the amount of watermark information that is disguised into have sound yet not at the expense of impalpability. According to IFPI, payload ought to be in excess of 20 bps. Security alludes that approved people can have the option to acquire the watermark. Watermarked signs ought not uncover any pieces of information in regards to the watermarks that are hidden in them. This can be accomplished through mystery keys which scrambles the watermark. At long last, the structured DAW plans should have less computational unpredictability.

These DAW plans require have sound alongside watermarked sound for watermark extraction. Creators in (Erçelebi and Batakçı, 2009), proposed a DAW plot utilizing

Lifting-Based Wavelet Transform (LBWT). PN arrangement is utilized to create watermark what's more, is embedded in Low Frequency (LF) parts of LBWT deterioration. Decision of LF parts gives better impalpability. Synchronization assaults are not investigated by the creators.

H. H. Yee et al., (Yee and Wei, 2009) proposed a strategy to encode watermark with cyclic code and afterward inserted into the host sound. The exhibition of this work (Yee what's more, Wei, 2009) is assessed on sound system signals against four SP assaults. The creators guarantee that 100% recuperation of the watermark is conceivable significantly under assaults.

Creators proposed a viable DAW conspire dependent on DWT in (Al-haj et al., 2011). Watermark is disguised in HH coefficients of host sound and the presentation is assessed against stirmark assaults. Impalpability is above 20dB as expressed by IFPI.

Sound watermarking is proposed in (Yassine et al., 2012) in light of two changes DWT and Discrete Sine Transform (DST). The DWT breaks down the host sound and afterward divided the estimate and detail coefficients into outlines and changed with the DST. Watermark is scrambled utilizing Finite Ridgelet Transform (FRIT) and afterward embedded in both guess and detail coefficients. The twofold inclusion of the watermark in low and high recurrence coefficient gave more flexibility to assaults. The calculation is tried against SP assaults on eight classes of mono sound and normal SNR is 25.51 dB.

Creators in (George, 2013) introduced a non-dazzle DAW conspire utilizing EMD and HHT. Trial results demonstrate that it meets the IFPI necessities. The plan has great flexibility against SP assaults, for example, MP3 and TSM assaults.

Non-daze DAW conspire utilizing DWT and SVD was introduced by A. Al-Haj (Al-Haj, 2014a). Creator tried the viability of the plan on three classes of sound viz., pop, instrumental, and discourse. This plan is hearty against some broad SP assaults and further work is to be conveyed to withstand desynchronization assault.

Creators in (Hemis and Boudraa, 2014) proposed a DAW plan to embed watermark in SVs got from the DWT LF coefficients of host sound. This extraction is a non-dazzle procedure and this plan utilized a twofold key for addition and extraction. The creators showed that the calculation has high strength against regular SP assaults.

In (Cichowski et al., 2015), creators proposed a technique to implant a10-character content data in DWT area. The work is assessed as far as emotional and target estimates which presume that it is less impervious to a few sorts of assaults. The creators situate themselves to improve the algorithm's heartiness against other SP assaults.

III. PROPOSED METHODOLOGY

The implanting procedure is executed in the accompanying advances and can be seen in Figure 3.

Stage 1: Perform DWT on unique signal A. This activity produces two sub bands: A_T and D_T. Here D_T represents to the Details sub-band, and A_T speaks to the estimation sub-band.

Stage 2: Apply Arnold Transform to watermark image.

Stage 3: Embed the mixed watermark into the DWT changed unique signal.

This can be accomplished by the accompanying Equation (1).

$$A_W = A_T + (\alpha * W) \quad (1)$$

Where, α is a Scaling factor and it is chosen such that audio quality is not degraded.
A_T is the transformed audio signal.
W is the scrambled watermark image.
A_W is the watermarked signal.

Step 4: Apply the inverse DWT operation to obtain watermarked.

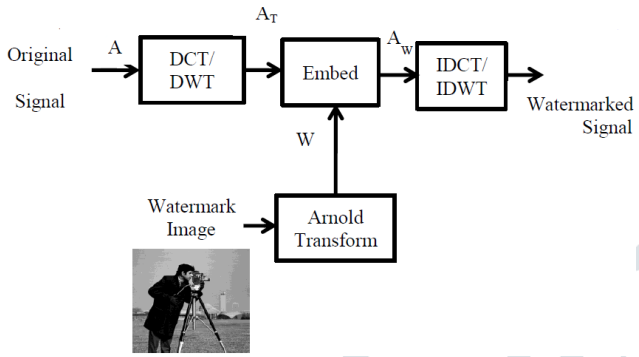

Fig. 3: Watermark concealing process of proposed DW

Watermark Extraction

The extraction process is implemented in the following steps and is represented in Figure 4.

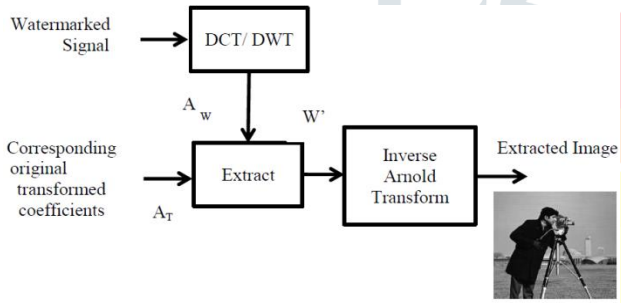

Fig. 4: Watermark extraction process of proposed DW

Step 1: Perform DWT on watermarked signal.
Step 2: Obtain the DWT coefficients of the original signal.
Step 3: Transformed watermark can be obtained by using the following Equation (2).

$$W' = \frac{A_W - A_T}{\alpha} \quad (2)$$

Where, W' is the scrambled watermark.
Step 4: Perform inverse Arnold Transform operation to obtain the extracted watermark gray image.

Applications of DW

Utilizations of DAW plans are copyright security, observing, fingerprinting, sign of substance control, data bearer, get to control, etc.

Copyright security: - Copyright holder inserts proprietorship data as watermark and this ought to be secure and vigorous against SP/DS assaults. It empowers the proprietor to build up evidence of possession if there should arise an occurrence of debate.

Monitoring: - Camouflage of watermark empowers following of unlawful duplicating

Fingerprinting: - A few highlights/characteristics of a sound are utilized as unique mark and embedded in have sound. This fingerprinting application is helpful for following the cause or beneficiary of a particular duplicate. All in all, watermarks with various sequential codes are embedded in sound CDs/DVDs preceding their appropriation.

Indication of substance control: - Content controlled due to SP/DS assaults by outsiders purposefully or unexpectedly can be recognized through a delicate watermark.

Information bearer: - Watermark embedded can give data with respect to copyright or permitting subtleties. Embedded metadata may convey data about classification of music, soloist and arranger and so forth.

Access Control: - Embedded watermark acts like a trigger, and enables the gadget to play the substance or not.

Parameter

Normalized Correlation coefficient (NC)

It states correlation between original watermark *W* and extracted watermark *W'*, which is shown in Equation (3):

$$NC = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} W(x,y)W'(x,y)}{\sqrt{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} W^2(x,y)}\ \sqrt{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} W'^2(x,y)}} \quad (3)$$

Where, x and y are spatial coordinates.

Peak Signal to Noise Ratio

If watermark is gray image then, to determine the degradation of the original image, the Peak Signal to Noise Ratio (PSNR) can be used.

$$PSNR = 10\log_{10}\left(\frac{x^2}{MSE}\right) \quad (4)$$

Where, x is the maximum intensity variation in image

IV. CONCLUSION

In this section, the recreation results approve that the proposed DW plans are profoundly indistinct and strong. The proposed DW (DCT) installs the watermark in the most noteworthy vitality coefficients. Vitality compaction property of DCT is misused to accomplish more strength. This proposed DAW (DCT) is flexible against assaults viz., resample, low pass channel, re-quantization, irregular clamor and AWGN.
In all the three proposed plans, watermark is implanted in the underlying coefficients of the changed host sound. This influences just the couple of coefficients of the watermarked which bring about high indistinctness. Yet, these plans can't avoid DS assaults as numerous duplicates of watermark are absent in watermarked sound.

REFERENCE

[1] Awdhesh K. Shukla, Akanksha Singh, Balvinder Singh and Amod Kumar, "A Secure and High-Capacity Data-Hiding Method using Compression, Encryption and Optimized Pixel Value Differencing", IEEE Access, October 8, 2018.

[2] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption", IEEE , 2018.

[3] N. Senthil Kumaran, and S. Abinaya, "Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique", International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[4] Aase, S.O., Husoy, J.H. and Waldemar, P. (2014) A Critique of SVD-Based Image Coding Systems, IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, Pp. 13-16.

[5] Ahmed, F. and Moskowitz, I.S. (2014) Composite Signature Based Watermarking for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp.1-8.

[6] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C. (2013) Blind Image Watermarking Using a Sample Projection Approach, IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, Pp.883-893.

[7] Ali, J.M.H. and Hassanien, A.E. (2012) An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, Advanced Modeling and Optimization, Vol. 5, No. 2, Pp. 93-104.

[8] Baaziz, N., Zheng, D. and Wang, D., "Image quality assessment based on multiple watermarking approach", IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), Hangzhou, Pp.1-5, 2011.