A Nested Digital Watermarking Scheme Using GARN with DWT

¹Edward Yellakour Baagyere, ²Peter Awonnatemi Agbedemnab, ²Mohammed Akolgo and ²Strato Angsoteng Bayitaa

¹Department of Computer Science, School of Computing and Information Sciences, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana

²Department of Information Systems and Technology, School of Computing and Information Sciences, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana

Article history Received: 18-03-2024 Revised: 26-05-2024 Accepted: 29-05-2024

Corresponding Authors: Peter Awonnatemi Agbedemnab Department of Information Systems and Technology, School of Computing and Information Sciences, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana Email: pagbedemnab@cktutas.edu.gh

Introduction

Over the years, the internet has developed and gained much popularity just as digital video content has gained ground in all aspects of human endeavors, which is mostly now being distributed over the internet. Notwithstanding, piracy of videos on the internet is also on the ascendency and this conundrum has had serious implications for copyright owners of online video content. Evidence exists that digital multimedia content such as images, text and videos can easily be altered and transmitted, which, poses a major threat to multimedia content creators as they become skeptical about the safety of their content online.

Since it has been established that piracy infringement is a major issue as far as the development of the video industry is concerned (Asikuzzaman and Pickering, 2018), there is therefore, a need for continuous research and development of new techniques that can assure copyright protection.

A popular traditional copyright protection technique over the years has been cryptography; this involves the use of secret characters to communicate a message. In cryptography, information is processed using either a symmetric key or a public key with high scrutiny. The original text is scrambled into what is known as cipher text, then back again upon arrival at the recipient's end. The attacker only sees the scrambled text but cannot

Abstract: Copyright infringement is undoubtedly one of the major challenges in the film and TV industries over the years but has become even more pervasive lately as a result of technological advancement. This has made it possible to decode hitherto, hard-encoded, or encrypted multimedia content resulting in a lot of losses to companies in such industries. Digital watermarking, which is, a process of embedding a piece of code or information in multimedia elements either covertly or visibly to provide copyright information is one way to show proof of ownership when taking legal action against an infringement. That is, digital watermarking can play a very important role in copyright protection. Also, it is possible to encrypt some copyright information to make it unreadable to adversaries who might reveal what has been watermarked. This study presents a nested digital watermarking scheme that utilizes the crossover and mutation properties of a Genetic Algorithm (GA) and leverages the chaotic nature of the Residue Number (RN) System (RNS) to encrypt a covert image. Furthermore, this encrypted image is invisibly embedded in a video by decomposing the video into frames using the Discrete Wavelet Transform (DWT). Thus, we perform image watermarking after which, we perform the video watermarking using the watermarked image which in itself is ciphered thereby, making it a nested process. The encrypted image can contain hidden information that is not visible to attackers who may attempt to distort its content if it is discovered in order to prevent legal suits against copyright infringement. An analysis of the simulated results reveals that the proposed nested watermarked scheme modestly outperforms similar existing schemes in terms of perceptibility and robustness.

Keywords: Copyright Infringement, Film Industry, Discrete Wavelet Transform (DWT), Encryption, Genetic Algorithm (GA), Residue Number System (RNS), Watermarking

decipher the information. However, the frequent transmission of meaningless codes between two communication sides draws the attention of attackers who then become the target. Once the attacker is able to crack the cipher text, then the information will be available. It is against this backdrop that information-hiding technology which has the ability to disguise transmitted information from the attacker is utilized (Agbedemnab *et al*., 2019). The science of hiding information is steganography, where a carrier or a host carries some other information in a manner that will not be visible by mere visual analysis, (Baagyere *et al*., 2020). Digital watermarking employs similar techniques to steganography to embed data covertly in noisy signals such as texts, images, or videos. Digital watermarking can be classified as visible or invisible: Visible watermarking is perceptible to the human eye as observed by television stations or online video content portals where a trademark of the name is visible to everyone (Su *et al*., 1998). However, there are other times when content creators may not want their copyright stamps or trademarks to be visible, in this case, they employ invisible watermarking where the watermarked content is not perceptible to the human eye but further analysis can reveal the contents which, are mostly trademarks.

The utilization of certain operators associated with the Genetic Algorithm (GA) such as selection, crossover and mutation can be leveraged to build robust schemes in order to hide vital information for the purpose of watermarking. The GA is a search algorithm based on the mechanics of natural selection and natural genetics. It belongs to the family of evolutionary algorithms, along with genetic programming, evolution strategies and evolutionary programming. Its application in information security has been harnessed over the years, in particular on schemes for data encryption and hiding (Baagyere *et al*., 2020). The Residue Number System (RNS) has also gained prominence for its parallelism and decomposition of larger weighted integers into smaller residues through a chaotic process of unconventional conversions namely, forward conversion and reverse conversion. The uniqueness of the representation of RNS, coupled with its laborious arithmetic processes and conversions make the RNS a useful system for data security and has found widespread usage in cryptography over the years. Wavelet Transform is also a technique that can be employed in digital image processing, watermarking and compression, among other technologies of data security (Ram, 2022). The transforms are usually based on the wavelet, which is a mathematical function, of varying frequency and limited duration. The properties of the wavelet are capable of decomposing an original signal into wavelet transform coefficients. The original signal can be reconstructed by performing an Inverse Wavelet Transformation on these coefficients;

these transforms can either be continuous or discrete, (Debnath *et al*., 2017). This study leverages the inherent properties of the RNS as well as the evolutionism operators of GA to encrypt and hide information in an image which is further hidden in a nested manner using a video by applying the Discrete Wavelet Transform, (DWT). The objective is to develop an algorithm (scheme) that is robust yet imperceptible and very fast to much up with current computing needs. The rest of the paper is structured respectively as for a discussion of some related works, a detailed presentation of the proposed scheme, results from the simulation and analysis of the proposed scheme with existing schemes and a formal conclusion.

Related Work

A nested watermark is a watermark inside another watermark. This concept or procedure seeks to increase the capacity of the watermark in order to enhance the imperceptibility of the covert multimedia, (Bhalla and Nagrath, 2013). Many video watermarking schemes have been proposed by various researchers using various techniques to conceal secret information in a video in order to prove ownership by content creators. Li (2009) proposed a DWT and GA approach to video watermarking. A three-level DWT (3-DWT) was applied to the video frames after scene analysis. Genetic Algorithm was used to insert the watermark image which was scrambled using the Arnold scrambling algorithm. This was to ensure that the hidden data or watermark was not visible. However, the traditional Arnold scrambling technique only applies to the square area which constitutes a drawback of the scheme. Another scheme by (Agrawal and Khurshid, 2014) proposed a DWT and GAparticular swarm optimization-based watermarking for videos using an audio watermark scheme that embeds invisible watermark information into the video streams of MPEG-2, H.264/AVC, MPEG-4 standards. The shot segmentation technique was applied to the original input video sequence and segmented into a number of nonoverlapping shots with a number of frames identified. The audio watermark was converted into a 9-bit plane using bit plane slicing. The blue channel from the RGB video component was selected for embedding because it is more resistant to changes as compared to the red and green channels. The DWT was applied to each frame to divide the frames into sub-bands where the 9-bit plane sliced audio watermark was then embedded in the HL and LH sub-bands. The tradeoff between transparency and robustness was optimized using GA-particle swarm optimization. Even though the PSO is suitable for dealing with problems of large dimensions, the approach lacks a solid mathematical foundation for analysis to overcome practical multidimensional problems.

Another scheme presented by Babatunde *et al*. (2016) proposed an algorithm for a residue-based video

encryption scheme. The scheme takes a video and clip and determines its size in order to compress using the MPEG-IV compression algorithm which comes with the size of the compressed file. The compression ratio was computed and frames were extracted from the compressed video. The frames are supposed to be converted into pixels' values and passed through RNS using the moduli set $\{2^n\}$ $-1, 2^n, 2^n +1$ } to get the encrypted video. Although the products of MPEG are very high in quality, it results in a low compression ratio. Moreover, a large file may take longer to open thereby increasing the extraction time. The work by Meenakshi *et al*. (2014) also proposed a video watermarking technique using a slant transform. In this scheme, the video was converted into frames and the watermark was embedded in the slant transform domain by modifying the transform coefficients. The watermarked image was scrambled using key PN1 to generate a pseudorandom sequence and rounded to get the binary sequence of 72×88. An Exclusive-OR (XOR) was then performed between the binary sequence and the watermark. The hosted video was converted from RGB to YUV and the watermark was embedded in the luminance while the chrominance was untouched. The scheme utilises a single key for the encryption process which can limit the robustness of the scheme. Finally (Karpe *et al*., 2013) introduced a hybrid digital video watermarking scheme based on DWT and Principal Component Analysis (PCA).

The video frames were converted from RGB to YUV and1-DWT was applied to the luminance (Y) component of each of the frames. The binary image was then embedded into the low-level frequency sub band. The PCA was utilized to reduce the correlation among the wavelet coefficients as a result of the wavelet decomposition. However, when the number of principal components is not carefully selected, some information can be lost. Some other works by Juneja and Bansal (2019); Al-Gindy *et al*. (2022); Li *et al*. (2019); Asikuzzaman *et al*. (2022) employed different techniques to embed one multimedia content or another into a covert video. However, whilst imperceptibility has been the major target, modern digital devices are able to break such schemes. Therefore, if the content is ever discovered but is encrypted then it becomes difficult to decipher the meaning of the hidden content more so if the algorithms deployed in the encryption are robust enough to withstand prequantum adversarial attacks.

The proposed scheme takes a watermarked image' as presented in Agbedemnab *et al*. (2023) but in this case, changes that image to another called 'fire cherry' to be the covert image and a video named 'athletic' as the host. The 'athletic' video is converted into frames at every 10-sec interval to obtain a number of frames depending on the duration of the video. These frames are then decomposed into 3-DWT to obtain the LL3, LH3, HL3 and HH3 sub bands. Thereafter, the watermarked image is embedded into each of the frames.

This is to ensure that the watermark is distributed across the length of the video to improve robustness. It is also to investigate whether scene structure could have an influence on performance measures such as the Structural Similarity Index Measure (SSIM). The primary contributions of the paper are:

- i. Development of a nested watermarking algorithm for enhanced security for players in the film and TV industries
- ii. Analysis of the perceptibility rate and computational time complexity of the proposed algorithm
- iii. Evaluation and comparison of the proposed technique to existing ones for data security

The various notations and symbols used in the paper are shown in Table 1.

Materials and Methods

The proposed scheme which includes the algorithm, tools methods and procedure employed is presented in this section. The scheme embeds a watermarked image as the final product from Agbedemnab *et al*. (2023) into a video to further enhance the security of the information. The host video is denoted by H_v in the scheme whilst the watermarked image from Agbedemnab *et al*. (2023) is denoted by *Wmi*. The watermarked video obtained shall be denoted by *Wvid*. Figure 1 is a flow diagram that describes the embedding process of the proposed scheme. The frames of the video are extracted at time intervals of 10, 20, 30, 40, 50 and 60 sec. These frames together with the watermarked 'fire cherry' image are decomposed into 3-DWT to obtain LL3, LH3, HL3 and HH3 sub bands. The watermark is then embedded into the LL3 sub bands of each of the frames using Eq. (1):

$$
W_{\text{vid}} = (k * H_i) + (q * W_{\text{im}})
$$
\n(1)

Edward Yellakour Baagyere *et al.* / Journal of Computer Science 2024, 20 (10): 1214.1221 **DOI: 10.3844/jcssp.2024.1214.1221**

Fig. 1: Flow diagram of the embedding process

Next, we apply inverse DWT on the frames to obtain the watermarked frames. Finally, the extracted frames are recombined to form the nested watermarked video.

Figure 2 is the flow diagram of the reverse order to get the watermarked image, that is describing the extraction process of the proposed algorithm. It is noticed from the diagram that frames of the watermarked video at the same time intervals are extracted which is then subjected to a 3-DWT along with frames of the host video and results in the watermarked image being extracted using the inverse DWT in Eq. (2):

$$
W_{im} = (W_{vid} - k * H_i) / q
$$
 (2)

After these processes, the algorithm for ciphering and extraction presented in Agbedemnab *et al*. (2023) is employed on the extracted watermarked fire cherry image to further extract the scrambled pepper and eventually reorder the pixels to obtain the original pepper image. The detailed processes are outlined next: The embedding process gets the Host video (Hv) and converts it into frames at time intervals (10, 20, 30, 40, 50, 60). This is to enable select six random frames where the watermark can be embedded.

Fig. 2: Flow diagram for the extraction process

Embedding Process

- 1. Get the Host video (H_v) and convert it into frames at time intervals (10, 20, 30, 40,50, 60). This is to enable select six random frames where the watermark can be embedded
- 2. Decompose video frames into 3-DWT
- 3. Decompose *Wmi* into 3-DWT
- 4. Embed the W_{mi} into the (H_v) using Eq. (1)
- 5. Merge the frames to form the watermarked video *Wvid*

Extraction Process

- 1. Get the Host video (H_v) as frames at time intervals (10, 20, 30, 40, 50, 60)
- 2. Get the watermarked video (*W*VID) as frames at time intervals (10,20,30,40,50,60)
- 3. Convert frames of both (*Hv*) and (*Wvid*) into 3-DWT
- 4. Extract the covered image *Wmi* from the video using Eq. (2)
- 5. The extracted *Wmi* then goes through the extraction process in scheme 1 to obtain the original 'pepper' image

Simulation

The proposed scheme was implemented using MATLAB® 2022a on a core i5 processor.

A summary of these processes is presented in Algorithm 1 as a pseudocode.

Algorithm 1: Pseudocode for Scheme

Data: Get a watermarked image (*W*MI) **Result:** *Convert* (Hv) ^{$-as$} \rightarrow *frames*^{$-at$} \rightarrow *time* = [10,20,30,40,50,60] **1** For *S_i* ← 0 **to** *nume*1(*time*) **if** *time*(*i*) = *v.duration* **then Output:** *v.CurrentTime* = *time*(*i*) −*read*→ *frames* − as → *frame*(*i*) **Output:** $[LL, LH, HH, HL] = dwt3(i, Hv)$ **Output:** [*LL*, *LH*, *HH*, *HL*] = *dwt*3(*i*, *Wmi*) **Output:** $W_{mLL3} = k * (H_{LL3}) + q * (W_{m};L13})$ **Output:** *Get IDWT of WmLL3* **2 end Result:** *Merge framesas* = *Wvid* /* Extraction Process */ **Data:** *Get watermarked video* (*Hv*) **Data:** *Convert* (*Hv*) \rightarrow ^{*as*}→*frames* \rightarrow ^{*at*}→*time* = [10, 20, 30, 40, 50, 60] **Data:** *Get a watermarked image* (*W*VID) **Data:** *Convert* (W_{vid})^{-as}→ *frames*^{-at}→*time* = [10, 20, 30, 40, 50, 60] **3 For** $Si \leftarrow 0$ to *nume*1(*time*) *if time*(*i*) = *v.duration* **then Output:** *v.CurrentTime* = *time*(*i*)−−*read*→ *frames* − as→ *frame*(*i*) $$ *HL*] ^{*-of*}→3-*DWT* **Output:** $[LL, LH, HH, HL] = d_{wt3}(i, W_{mi})$ **Output:** $W_{mLL3} = k * (H_{LL3}) + q * (W_{mILL3})$ **Output:** Get IDWTo fWmLL3

4 end

Result: $\frac{-\text{extract}}{\longrightarrow} W_{mi}\frac{-as}{\longrightarrow}(H_{wmv} - k * (Y_{LL3}))/q$

Embedding Process

In the proposed scheme the athletic video is taken through the conversion process to obtain the video as frames in the time intervals 10, 20, 30, 40, 50 and 60 seconds. The frames are then decomposed into 3-DWT and the covert image is embedded into these frames using Eq. 1. In order to balance the tradeoff between robustness and imperceptibility, the optimal scaling factors of $k = 0.99$ and $q = 0.009$ are used for the embedding process since these values produce a perfect blend of the images. Figure 3 is the experiment for the embedding process. From the experiment, the covert watermarked fire cherry image is embedded into each of the frames generated.

Extraction Process

The extraction process takes the watermark image *Wvid* through the conversion process to obtain the six images. The frames at every 10-second time interval are extracted and 3-DWT is applied to both the watermarked video and the host video. Equation 2 is then used to extract the covert image from the video. Figure 4 shows the extraction experiment conducted. It is clear from both the video frames and the extracted fire cherry image that degradation in terms of the quality of the images has not occurred.

Fig. 3: Experiment 1-embedding watermark fire cherry image into video frames

Fig. 4: Experiment 2-extracting watermark fire cherry image from video frames

Results and Discussion

The results of the simulation were assessed to ascertain the level of imperceptibility and robustness of the watermarked image. The performance of the proposed scheme was analyzed using visual and statistical metrics as follows.

Imperceptibility

- (a) PSNR and MSE analysis: In image watermarking, the quality of the image is measured based on the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) between the original frames and the watermarked frames. While the MSE represents the cumulative square error between the original frames and the watermarked frames, the PSNR denotes the measure of the peak error. A smaller value of MSE indicates minimal difference between the original and watermarked frames. A larger value of PSNR also shows minimal distortion in pixel values as shown in Table 2
- (b) *SSIM* analysis: The Structural Similarity Index Measure (*SSIM*) compares the similarities between the original and watermarked video based on luminance, contrast and structural similarity components. The structural similarity index is a combination of these components given (Wang *et al*., 2004):

$$
SSIM(x, y) = f(x, y), c(x, y), s(x, y))
$$
\n(3)

where, $l(x, y)$ is luminance comparison, $c(x, y)$ is contrast comparison and *s*(*x,y*) is structural comparison, (Thakur *et al*., 2010). The *SSIM* gains a value from 0-1, where 1 is the maximum quality. Therefore, an *SSIM* value of 1 shows that the original frames and watermark frames are exactly the same while a *SSIM* value of 0 indicates that the two images are not similar. The *PSNR* and *SSIM* values for the proposed scheme are presented in Table 2. The results of *SSIM* show that the original athletic and watermarked videos are very similar which indicates how imperceptible the watermark image is.

Robustness

To assess the robustness of the proposed scheme, some attacks were performed on the watermarked frames:

- (a) Resizing: The watermarked frames were resized from their original size of $1152\times720-576\times360$ pixels. The reduced image was then resized back to its normal size before the extraction. The extracted watermarked fire cherry image maintained its quality after going through this process
- (b) Motion blurring: The watermarked frame was subjected to motion blurring before the extraction procedure was conducted. This procedure had minimal effects on the image of the extracted watermarked fire cherry image
- (c) Gaussian noise: The watermarked frame is subjected to Gaussian noise with mean $= 0$ and $SD = 0.01$. The pixels of the watermarked fire cherry image saw some bit of distortion but was not enough to derail the extracted watermark image
- (d) Sharpening: The watermarked video is highpass filtered with a mask 3×3 . The extracted watermark image remained almost exactly the same as the original image
- (e) Salt and pepper: We introduced salt and pepper noise with a noise density of 0.01. Salt and pepper noise also had some minimal distortion on the extracted watermark but the image still possesses its qualities

Table 3 illustrates the results of the attacks on the frames and the structural similarity index measure between the original and extracted fire cherry.

Time Complexity

The main computation of the algorithms comes from the encryption process and the watermarking process. The computation maps with complexity $O(n)$ since the two main computations are conducted in a linear iteration of the input data. As the size of the image grows, the computational time increases accordingly. Therefore, the algorithms have a linear time complexity since the image size determines the amount of time needed to run it. The average processing time of the proposed schemes is shown in Table 3.

Performance Evaluation

The results obtained from the experiments conducted using the proposed scheme were also compared with existing similar state-of-the-art schemes. The scheme by (Thakkar and Srivastava, 2017) utilizes Compressive Sensing (CS) and Principle Components (PC) to develop the watermarking scheme while the works by Kothari and Dwivedi (2015) employ a hybridization technique that combines DCT, SVD and DWT to develop the scheme. The performance evaluation of the proposed scheme as compared to these schemes is presented in Table 4.

The performance of the proposed scheme is compared with similar existing schemes by Al-Gindy *et al*. (2022); Asikuzzaman *et al*. (2022) in terms of the imperceptibility measured using the PSNR and SSIM values and the time of execution. The time complexities of the compared schemes are not recorded but it is worthy of note that the use of RNS which employs the residues of numbers has significantly influenced the fastness of the proposed scheme. Also, as observed in Table 4, the proposed scheme performs favorably in terms of the PSNR and SSIM values. In the era of fast and cloud computing, it is imperative that schemes are lightweight and fast to be able to perform favorably. The choice of GA and RNS has put the proposed scheme in a better position for prequantum computing activities relating to digital watermarking.

Table 3: PSNR and SSIM values for the video frames after the attack

Attacks	Watermarked Frames	Extracted W _{mi}	SSIM
No Attack	10sec		0.9987
Resizing	20sec		0.7946
Motion Blurring	30sec		0.7890
Gaussian Noise	40sec Markinl		0.9941
Sharpening	50 _{sec}		0.9986
Salt and Pepper	60sec		0.9887

Edward Yellakour Baagyere *et al.* / Journal of Computer Science 2024, 20 (10): 1214.1221 **DOI: 10.3844/jcssp.2024.1214.1221**

Conclusion

The paper presented a nested digital watermarking scheme by leveraging the operators of GA and the chaotic and parallelism properties of the residue number system. The proposed scheme embeds a watermarked image into a video as the cover information and ensures that the watermark is spread across the entire video, making it robust. An attacker will not be able to detect and extract all watermarks within the video as there is some encryption of the hidden information. The proposed algorithm makes it difficult to perceive hidden content in a host, even so, the hidden media is robustly encrypted as presented in Agbedemnab *et al*. (2023) with data. Thus, the proposed combination is highly efficient as it enhances image security and imperceptibility.

Acknowledgment

The authors acknowledge the support provided by the Management of the University and that of the Google African PhD Fellowship Award.

Funding Information

This study was supported in part by a Google African PhD Fellowship Award.

Author's Contributions

Edward Yellakour Baagyere: Concept of work; presented and methodology; supervision; final proofreader.

Peter Awonnatemi Agbedemnab: Concept of work; presentation and methodology; choice of material, typesetter; proofreader.

Mohammed Akolgo: Original draft; programed and simulation, methodology and presented; choice of material; typesetter.

Strato Angsoteng Bayitaa: Programming and simulation, methodology and presented; choice of material; proofreader.

Ethics

Authors declare no conflict of interest. Also, all materials used in this article particularly images, are available online without copyright issues.

References

- Agbedemnab, P. A., Akolgo, M., & Agebure, M. A. (2023). A New Image Watermarking Scheme Using Genetic Algorithm and Residual Numbers with Discrete Wavelet Transform. *Journal of Information Security*, *14*(04), 422–436. <https://doi.org/10.4236/jis.2023.144023>
- Agbedemnab, P. A.-N., Baagyere, E. Y., & Daabo, M. I. (2019). A Novel Text Encryption and Decryption Scheme using the Genetic Algorithm and Residual Numbers. *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019*, 1–9. <https://doi.org/10.29007/zd9h>
- Agrawal, P., & Khurshid, A. (2014). DWT and GA-PSO Based Novel Watermarking for Videos Using Audio Watermark. In Y. Tan, Y. Shi, & C. A. Coello Coello (Eds.), *Advances in Swarm Intelligence: 5 th International Conference, ICSI 2014, Hefei, China, October 17-20, 2014, Proceedings, Part II 5 8795*, pp. 212–220). Springer, Cham. https://doi.org/10.1007/978-3-319-11897-0_25
- Al-Gindy, A., Omar, A. A.-C., Mashal, O., Shaker, Y., Alhogaraty, E., & Moussa, S. (2022). A new watermarking scheme for digital videos using DCT. *Open Computer Science*, *12*(1), 248–259. https://doi.org/10.1515/comp-2022-0238
- Asikuzzaman, Md., & Pickering, M. R. (2018). An Overview of Digital Video Watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*, *28*(9), 2131–2153. <https://doi.org/10.1109/tcsvt.2017.2712162>
- Asikuzzaman, Md., Mareen, H., Moustafa, N., Choo, K.- K. R., & Pickering, M. R. (2022). Blind Camcording-Resistant Video Watermarking in the DTCWT and SVD Domain. *IEEE Access*, *10*, 15681–15698. <https://doi.org/10.1109/access.2022.3146723>
- Baagyere, E. Y., Agbedemnab, P. A.-N., Qin, Z., Daabo, M. I., & Qin, Z. (2020). A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers. *IEEE Access*, *8*, 100438–100447. <https://doi.org/10.1109/access.2020.2997838>
- Babatunde, A. N., Jimoh, R. G., & Gbolagade, K. A. (2016). An algorithm for a residue number systembased video encryption system. *Computer Science Series Journal*, *14*(2), 136–147. [http://anale-informatica.tibiscus.ro/download/lucrari/14-2-](https://doi.org/http:/anale-informatica.tibiscus.ro/download/lucrari/14-2-19-Babatunde.pdf) [19-Babatunde.pdf](https://doi.org/http:/anale-informatica.tibiscus.ro/download/lucrari/14-2-19-Babatunde.pdf)
- Bhalla, J. S., & Nagrath, P. (2013). Nested digital image watermarking technique using blowfish encryption algorithm. *International Journal of Scientific and Research Publications*, *3*(4), 1–6.

[https://citeseerx.ist.psu.edu/document?repid=rep1&t](https://doi.org/https:/citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1752f10bf93e9011c011d8d2c1ae056d2d0deace#page=386) [ype=pdf&doi=1752f10bf93e9011c011d8d2c1ae056](https://doi.org/https:/citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1752f10bf93e9011c011d8d2c1ae056d2d0deace#page=386) [d2d0deace#page=386](https://doi.org/https:/citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1752f10bf93e9011c011d8d2c1ae056d2d0deace#page=386)

- Debnath, Lokenath, & Shah, F. A. (2017). *Lecture notes on wavelet transforms* (1 st Ed.). Birkhäuser Cham. <https://doi.org/10.1007/978-3-319-59433-0>
- Juneja, K., & Bansal, S. (2019). Frame Selective and Dynamic Pattern Based Model for Effective and Secure Video Watermarking. *International Journal of Computing*, *18*(2), 207–219. <https://doi.org/10.47839/ijc.18.2.1419>
- Karpe, K. S., Shah, D. S., & Mukherji, P. (2013). Hybrid Digital Video Watermarking based on DWT-PCA. *International Journal of Advance Research in Computer Science and Management Studies*, *1*(5), 118–127.
- Kothari, A. M., & Dwivedi, V. V. (2015). Video Watermarking–Embedding binary watermark into the digital video using hybridization of three transforms. *International Journal of Signal and Image Processing Issues*, *2015*(1), 9–17.
- Li, L. Z. A. (2009). A Study on Video Watermark Based-on Discrete Wavelet Transform and Genetic Algorithm. *2009 1st International Workshop on Education Technology and Computer Science*, 374–377. https://doi.org/10.1109/etcs.2009.611
- Li, Z., Chen, S. Q., & Cheng, X. Y. (2019). Dual Video Watermarking Algorithm Based on SIFT and HVS in the Contourlet Domain. *IEEE Access*, *7*, 84020– 84032. <https://doi.org/10.1109/access.2019.2899378>
- Meenakshi, K., Srinivasa Rao, Ch., & Satya Prasad, K. (2014). A Scene Based Video Watermarking Using Slant Transform. *IETE Journal of Research*, *60*(4), 276–287.

<https://doi.org/10.1080/03772063.2014.961570>

- Ram, B. (2022). Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform. *SSRN Electronic Journal*, 1–7. <https://doi.org/10.2139/ssrn.4173742>
- Su, J. K., Hartung, F., & Girod, B. (1998). Digital watermarking of text, image and video documents. *Computers and Graphics*, *22*(6), 687–695. [https://doi.org/10.1016/s0097-8493\(98\)00089-2](https://doi.org/10.1016/s0097-8493(98)00089-2)
- Thakkar, F. N., & Srivastava, V. K. (2017). A fast watermarking algorithm with enhanced security using compressive sensing and principle components and its performance analysis against a set of standard attacks. *Multimedia Tools and Applications*, *76*(14), 15191–15219.

https://doi.org/10.1007/s11042-016-3744-0

- Thakur, M. K., Saxena, V., & Gupta, J. P. (2010). A performance analysis of objective video quality metrics for digital video watermarking. *2010 3rd International Conference on Computer Science and Information Technology*, 12–17. https://doi.org/10.1109/iccsit.2010.5564962
- Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Transactions on Image Processing*, *13*(4), 600–612. https://doi.org/10.1109/tip.2003.819861