Scientific Research Publishing

Journal of Information Security, 2023, 14, 422-436
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A New Image Watermarking Scheme Using Genetic Algorithm and Residual Numbers with Discrete Wavelet Transform

Peter Awonnatemi Agbedemnab[1], Mohammed Akolgo[1], Moses Apambila Agebure[2]

[1]Department of Information Systems and Technology, School of Computing and Information Sciences, C.K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana
[2]Department of Computer Science, School of Computing and Information Sciences, C.K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana
Email: pagbedemnab@cktutas.edu.gh, zugah1985@gmail.com, magebure@cktutas.edu.gh

How to cite this paper: Agbedemnab, P.A., Akolgo, M. and Agebure, M.A. (2023) A New Image Watermarking Scheme Using Genetic Algorithm and Residual Numbers with Discrete Wavelet Transform. *Journal of Information Security*, **14**, 422-436.
https://doi.org/10.4236/jis.2023.144023

Received: July 3, 2023
Accepted: October 15, 2023
Published: October 18, 2023

Copyright © 2023 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Transmission of data over the internet has become a critical issue as a result of the advancement in technology, since it is possible for pirates to steal the intellectual property of content owners. This paper presents a new digital watermarking scheme that combines some operators of the Genetic Algorithm (GA) and the Residue Number (RN) System (RNS) to perform encryption on an image, which is embedded into a cover image for the purposes of watermarking. Thus, an image watermarking scheme uses an encrypted image. The secret image is embedded in decomposed frames of the cover image achieved by applying a three-level Discrete Wavelet Transform (DWT). This is to ensure that the secret information is not exposed even when there is a successful attack on the cover information. Content creators can prove ownership of the multimedia content by unveiling the secret information in a court of law. The proposed scheme was tested with sample data using MATLAB2022 and the results of the simulation show a great deal of imperceptibility and robustness as compared to similar existing schemes.

Keywords

Discrete Wavelet Transform (DWT), Digital Watermarking, Encryption, Genetic Algorithm (GA), Residue Number System (RNS), GARN

1. Introduction

The internet provides the opportunity for people to copy, process and transmit multimedia content including text, graphics, images and videos, making it easy

and convenient for content creators to market their products to clients. However, acts by some individuals such as piracy, infringement and stealing of online content tend to damage intellectual property rights and affect the market order of content owners [1]. This, therefore, makes it necessary to employ techniques for information hiding. Information hiding is the process of embedding a secret message into cover content in order to make the information imperceptible and conceal the existence of the secret message [2]. Information hiding includes steganography, digital watermarking and convert communication. Among these three technologies, digital watermarking is the best solution to copyright protection for digital content [3]. Digital watermarking is the ability to embed information (either visible or invisible) into the cover information [4]. Digital watermarking can be classified based on the domain for spatial or spectral; the type of document for text, image, audio or video; or human perception for robust and fragile [5]. There exist various forms of attacks (active, passive collusion, forgery and so on) on watermarks. More prevalent are these attacks recently as a result of the growth in the digital ecosystem especially, internet technology. Attempts have been made over the years to handle these attacks by building robust watermark schemes. Indeed, robustness is a requirement for digital watermarking. However, in order to achieve robustness, there has always been a trade-off with imperceptibility. Imperceptibility and robustness can be achieved by leveraging techniques that can bring imperceptibility but at the same time increase the computational layers to build robust schemes. This paper, therefore, seeks to proffer a solution to these threats in the modern era by leveraging the selection and crossover operators of the genetic algorithm (GA) and at the same time, the inherent properties of the residue number system (RNS) to encrypt an image before it will be embedded in a cover image using a three-level Discrete Wavelet Transforms (3-DWT). The rest of the paper is organised as follows: Section 2 presents the necessary background information as well as a review of some related works; the proposed scheme is presented in Section 3. The results of the scheme are analysed in Section 5 as well as an evaluation of its performance whiles Section 3 concludes the paper.

2. Background and Related Works

Watermarking is a technique that has been in existence for several centuries now. Watermarks were found initially in plain paper and in paper bills. However, digital watermarking emerged in recent years [5] [6]. The main purpose of digital watermarking is for copyright protection, so that when pirated products emerge, content owners are able to extract some hidden information in the content to prove ownership of the content in a court of law [7].

GA is a search technique used to find true and approximate solutions to optimisation and search problems. It forms part of the Evolutionist Algorithm (EA) category which makes use of evolution theory in solving problems. These algorithms are biologically inspired because they mimic how living creatures try to

fit into their environment for survival. The basic operators of GA are selection, crossover and mutation. It begins with the selection of chromosomes from a population of chromosomes which undergoes modification (recombination and mating) to form a new population. GAs have seen significant applications in solving complex real world computation problems including Neural networks, Vehicle routing problems, and Task scheduling among others.

A residue number system (RNS) is a number system that represents integers as a vector of remainders of a given pairwise co-prime integers called the moduli. The residue number system is a non-weighted number system which is different from the weighted number systems like binary or decimal number systems. This number system possesses inherent properties such as parallelism, fault tolerance, and modularity that make it suitable for application in many research areas. RNS has been widely applied in the area of subtraction, multiplication and addition such as Digital Signal Processing (DSP) due to its computational speed. However, it has not gained much popularity in areas of division such as Signal Detection, Magnitude Comparison and Overflow Detection [8]. Given a set of relatively prime moduli $S=\{m_1,m_2,\cdots,m_n\}$, such that the greatest common divisor (gcd) between any pair is one, *i.e.* $gcd(m_i,m_j)=1$, for $i\neq j$. We can compute $M=\prod_{i=1}^{n}$, where S and M are the base and the dynamic range of the RNS respectively. In the RNS, any number X which is less than M can be denoted as a vector $X=x_1,x_2,\cdots,x_n$, where $x_i=|X|_{m_i}$. Such an integer X is a legitimate number and has a unique representation within the dynamic range, M [9]. Assume that two integers $X,Y\in[0,M)$ for RNS representation are $X=\{x_1,x_2,\cdots,x_n\}$, and $Y=\{y_1,y_2,\cdots,y_n\}$, respectively. With a single step, we can compute $X\phi Y=\left(|x_1\phi y_1|_{m_1},|x_2\phi y_2|_{m_2},\cdots,|x_n\phi y_n|_{m_n}\right)$ where ϕ denotes an addition, subtraction, or multiplication. This property provides parallel operation on all digits without any carry between different residue digits [9].

Forward conversion in RNS refers to the decomposition of a weighted number into RNS representation. This process is relatively a straight forward operation where modulus operation is performed on the weighted number with respect to the moduli set. For example, given a moduli set $S=\{m_1,m_2,\cdots,m_n\}$, then the weighted number (in this case, binary or decimal) is represented in RNS as $X=|x|_{m_i},i=1,2,3,\cdots,n$. The reverse (RNS-to-binary/decimal) conversion on the other hand is a more complex operation which is computed generally by two techniques; the Chinese Remainder Theorem (CRT) and the Mixed Radix Conversion (MRC).

The CRT is computed as [10];

$$\left|\sum_{i=1}^{N} m_i\left|x_i a_i\right|_{m_i}\right|_M \tag{1}$$

where,

$$M=\prod_{i=1}^{N} m_i;\ a_i=\frac{M}{m_i};\ |x_i\cdot a_i|_{m_i}=1$$

Wavelet Transform is a modern technique which is recently being used in digital image processing, watermarking, compression, and other applications, [11]. The transforms are based on the wavelet of varying frequency and limited duration. A wavelet is a mathematical function that is used in image processing. Wavelets consist of two fundamental properties: scale and location. The scale refers to how stretched or "squeezed a wavelet is. Location defines where the wavelet is positioned in time. 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. There are two types of Wavelet Transforms, Continuous Wavelet Transform (CWT) and DWT [12].

Many researchers have proposed various schemes for digital image watermarking by combining GA and other techniques or RNS and other techniques. The work by [13] presented a Wavelet-Hadamard GA and decision tree-based image watermarking scheme. The GA was used in the search for optimization to satisfy the tradeoff between robustness and imperceptibility. According to the proposed scheme, embedding a secret image into a cover image will involve a modification of the frequency coefficients. The paper, therefore, utilized GA to modify the coefficients of the host image. However, this technique was proven to be convenient for only offline applications and cannot withstand attacks when applied to online content. Another work by [14] also presented a watermarking technique that is based on Redundant Wavelet Transform (RWT) and the GA. In this work, RWT is employed to reduce the information loss in the extracted image as this is the case, according to the paper in conventional wavelet transforms. The GA was used here to optimize a watermarking constant. The approach achieved resilience towards attacks but it is costly in terms of computational time. Also, [15] reported on a digital signature-based watermarking scheme which uses integer wavelet transform and singular value decomposition. The proposed approach employed two algorithms, GA and Particular Swarm Optimisation (PSO). The signature generation and embedding procedure was based on singular values. However, the approach adopted a lot of methods which introduced computational complexities and delays in the execution time. Again, [16] also established a coding scheme which can be used to insert data into an image and to extract the data from the image without changing the image file. This scheme is established based on Discrete Cosine Transform (DCT) and GA. In their work, the cover image is decomposed into 3-level using DCT then GA is used for the embedding process. However, the problem with DCT is that images are broken into blocks of 8×8, 16×16 or bigger. Therefore, when the image is reduced to higher compression ratios, the blocks become visible.

The work in [17] resorted to the use of Data Encryption Standard (DES) and RNS for image watermarking. The secret image was taken through a Simple-DES (SDES) using a key image, then the encrypted image was watermarked using another image and a matrix. The work then applied RNS to produce a DES wa-

termarked RNS encoded image. The scheme showed some form of robustness but utilized only one key. The scheme in [18] proposed a high payload watermarking using RNS. The proposed approach takes pixel values from three watermarked images and embeds them into the cover image. The researchers converted the colour image into 3 gray planes (Red, Blue and Green) and applied RNS on the Blue plain and went further to do more RNS arithmetic on the bits of the chosen plain in order to watermark. This is, however, a single layer scheme since it utilizes only residue numbers for the watermarking process. Also, the work by [19] discussed the use of Advance Encryption Standard (AES) with a hybrid of DWT and DCT watermarking techniques and RNS for image watermarking. In this work, a grayscale image is given as an input to AES-128 using a key. The output is then watermarked using DWT and DCT and the watermarked image is then passed through the RNS procedure for security. However, the AES technique has a simpler algebraic structure and encrypts every block the same way. Therefore, when an attacker succeeds in decrypting one block, it becomes simpler to get the remaining blocks. From the ensued, GA has been combined with other techniques in some cases, and the RNS has also been used with some other techniques as well. However, both the GA and RNS have not been utilized for watermarking. This paper, therefore, seeks to leverage both techniques and in addition, DWT to develop a robust watermark scheme without compromising on the throughput.

3. Proposed Scheme

The proposed scheme utilizes a combination of three techniques, namely, GA, RNS and DWT in a three-layered manner to achieve its objective. The RNS component comprises a forwarded and reverse conversion process, where the decimal/binary values are converted into residues using the moduli set $\left\{2^{n-1}-1, 2^n-1, 2^n\right\}$, where $m_1 = 2^n - 1$, $m_2 = 2^n$ and $m_3 = 2^{n-1} - 1$; the residual bits are then used in the choice of pixel vectors for single point crossover operations and embedding using a 3-DWT. These are the encoding processes that result in the pixel scramble (encryption), which is eventually watermarked. The decoding involves a reversal of these processes; the residual bits are converted back to the binary/decimal representation for the recomposition of pixel values of the original image. The moduli set for the RNS conversion processes and manipulation in [10] are adopted in this paper. Generally the encoding processes of the proposed scheme are as follows:

1. For any $M \times M \left(M = 2^n\right)$ image, extract pixel values
2. Given the moduli set $\left\{2^{n-1}-1, 2^n-1, 2^n\right\}$, choose n such that $DR = m_1 \times m_2 \times m_3$ in order that every pixel can be represented.
3. Find $E_{key} = R_{key} \bowtie \overline{R}_{key}$, $\overline{R}_{key}$ is a representation of $m_1 m_2 m_3$ in binary and of length 2^n. R_{key} is a random key for the purpose of encryption whilst E_{key} is the encryption key.
4. Determine 2^n subkeys, $S_{key(i)} \left(i = 1, \cdots, 2^n\right)$ by splitting E_{key} into equal

n-bits starting from the LSB.

5. Note that the pixels of the image forms a matrix starting from location 0 to location $2^n - 1$. The subkeys are then used as a selection criterion for crossover operation.

6. To further scramble the image, map bits in R_{key} to pixel locations from left to right; and compute RNS forward conversion on pixel locations where $R_{key} = 1$.

7. The residual values are then replaced with corresponding pixel values to form the new encrypted image.

8. Finally, to embed, decompose both host image and encrypted image of sizes $M \times M$ into four non-overlapping 3-DWT sub-bands as shown in **Figure 1**. Thereafter, use Equation (2);

$$W_{im} = \alpha H_{im} + \beta E_{im} \tag{2}$$

α and β are scaling factors for the host image and watermark respectively. The scaling factors are varied from 0.0 to 1.0 to get the optimal values for embedding the image [20]. As the value of α increases the value of β decreases so that the host image becomes more visible whiles the scrambled image becomes invisible.

And that for the decoding processes will be to find a reverse process for each stage of the encoding processes. Equation 3 is used to extract the encrypted image through to the RNS reverse conversion stage where the reverse converter in [10] is adopted.

$$E_{im} = \left(W_{im} - \alpha H_{im}\right) / \beta \tag{3}$$

These processes are summarised as a pseudocode in Algorithm 1.

The proposed scheme was simulated using MATLAB on a Core i5 processor. Firstly, the image referred to in this paper as "Pepper" was taken through the encryption process. The results of this experiment are shown in **Figure 2**. From the experiment, it can be observed that the image is totally distorted. Regarding the security of the image, the attacker will have to first know the moduli set used to generate the random key and how the GA process was conducted with the sub-keys obtained from the expanded key.

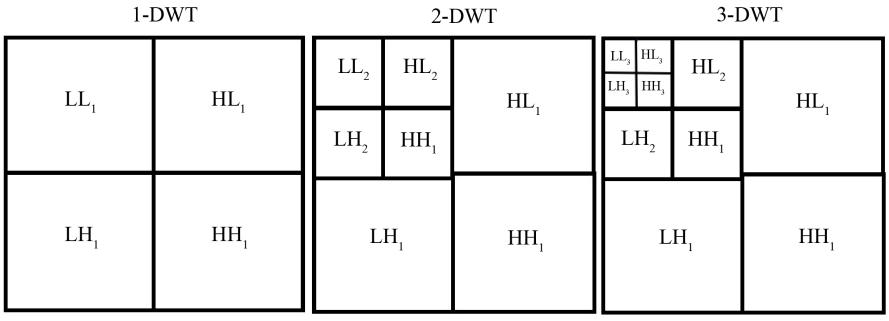

Figure 1. Illustration of DWT levels.

Algorithm 1: Pseudocode for Proposed Scheme

Data: Determine size of image and get all pixel values.
// Key generation
Result: Compute *dec2bin* (2^n-1, 2^n, 2^{n-1}-1) to obtain R_{key}
Result: $E_{key} = R_{key} \bowtie \overline{R}_{key}$
Result: Generate $S_{key(1)} \cdots S_{key(i)}$
// Block of keys
/* Scrambling Process */
while $V \leq N$ **do**
  repeat
    $S_{key(1)} : S_{key(i)}$
  until $temp = S_{key(1)}$
end
if $S_{key(1)} \neq S_{key(2)}$ **then**
  Swap($P_{[temp]}, P_{[S_{key(2)}]}$
  $temp = S_{key(2)}$
  for $S_{key(i)} \leftarrow S_{key(2)}$ **do**
    Next $S_{key(2)} + 1$
  end
end
for $S_{key(i)} \leftarrow 0$ **to** $(2^n - 1)$ **do**
  if $R_{key(i)} = 1$ **then**
    Output: $|P_v|_{mi}$
  end
end
Result: Store image as E_i
Result: Get H_i and $E_i \xrightarrow{decompose}$ as 3−DWT
/* Embedding Process */
Input: Embed in $LL_3 \xrightarrow{as} New_{LL3} = (k * H_{LL3}) + (q * E_{LL3})$
Result: Store image $\xrightarrow{as} W_{im}$
/* Extraction */
Result: Get H_i and $W_{im} \xrightarrow{decomposeas}$ 3−DWT
/* Watermark Extraction Process */
Output: Extract from $LL_3 \xrightarrow{as} New_{LL3} = (W_{im} - (k * H_{LL3}))/q$
Result: Store image $\xrightarrow{as} E_i$
/* Pixel Reordering Process */
while $V \leq N$ **do**
  repeat
    $S_{key(1)} : S_{key(i)}$
  until $temp = Skey(1)$
end
if $S_{key(1)} \neq S_{key(2^n)}$ **then**
  Swap($P_{[temp]}, P_{[S_{key(2^n)}]}$
  $temp = S_{key(2^n)}$
  for $S_{key(i)} \leftarrow S_{key(2^n)}$ **do**
    Next $S_{key(2^n)} - 1$
  end
end
for $S_{key(0)} \leftarrow 0$ **to** n **do**
  if $R_{key(i)} = 1$ **then**
    Output: $\overline{|P_v|}_{mi}$
  end
end
Result: Store image as original image

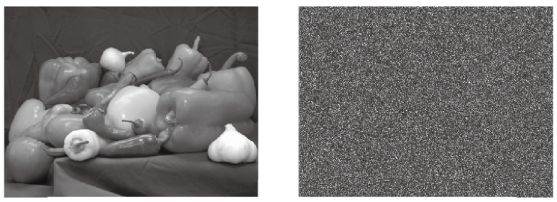

Figure 2. Encryption of image "Pepper".

Next, the encrypted image was embedded into the Host image, "Lena" using the Equation 2 with scaling factors, $\alpha = 0.99$ and $\beta = 0.009$ as shown in **Figure 3**. These scaling factors were chosen after conducting series of tests on

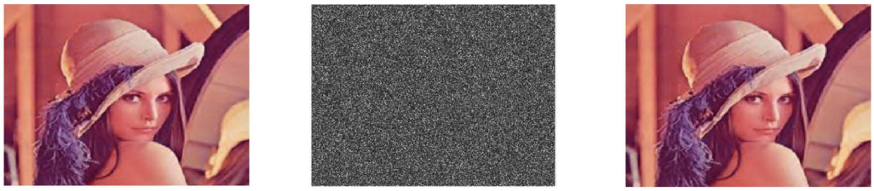

Figure 3. Watermarked image "Lena".

the two images by varying between 0.0 to 1.0. This provided a suitable blend of the two images and conceals the existence of the encrypted image and leaves no traces of suspicion to an attacker.

To extract the encrypted image from the host image, DWT is applied on both the watermarked image and host image and then alpha blending. Equation 3 is applied on the low frequency sub-bands of both images. After extraction, the inverse DWT is applied on the encrypted image. The encrypted image is then taken through reverse GA and RNS procedure to obtain the original image. **Figure 4** shows the experiment conducted on the extraction process. It is obvious that the decrypted image produced a similar image as the original and does not cause any distortion as a result of the encryption process.

4. Results Analysis

The results from the simulation of the proposed scheme were analyzed based on standard metrics on imperceptibility and robustness for watermarking schemes.

4.1. Visual Testing

As shown in **Figure 3**, it is obvious that the encrypted image looks very chaotic at sight and does not provide any clue that points to the original image. Therefore, it can be concluded that there are no perceptual similarities between the original image and the encrypted image. It can also be observed from **Figure 4** that the watermarked image is similar to the original "Lena" image from the human visual perspective and does not reveal any clue to the fact that there is an embedded image in it. The decrypted image in **Figure 5** also looks exactly the same as the original "Pepper", showing no form of distortion as a result of the encryption process.

4.2. Sensitivity Analysis

In order to affirm the claim that the encrypted image differ significantly from the original image, the following statistical measures were performed:

A. MSE and PSNR Analysis

The Mean Square Error (MSE) is the average of the squares of the "errors" between the original image and the encrypted image. The error is the measure of the extent to which the values of the original image differ from the encrypted

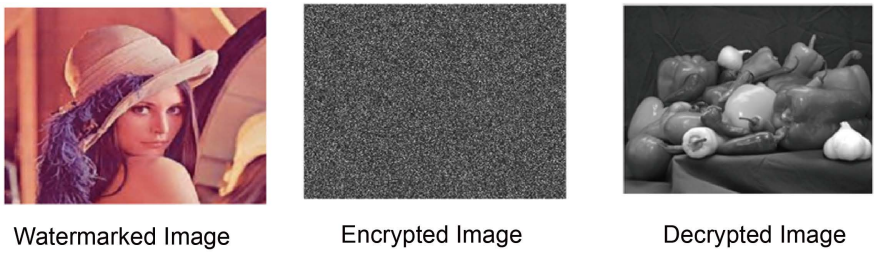

Figure 4. Extraction of encrypted image.

image. This can be represented mathematically as [1];

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{i=1}^{N} \left(P(i,j) - C(i,j) \right)^2 \tag{4}$$

where $P(i,j)$ represents the original image whiles C(i,j) represents the watermarked image, M and N are the number of rows and columns of the two images. The MSE values indicates the measure of the difference between the original and the watermarked image. The higher the MSE value, the larger the difference between the original image and the watermarked image and vice versa.

Peak Signal to Noise Ratio (PSNR) is an expression of the ratio of peak signal power to noise power. This can be represented mathematically as [3];

$$\text{PSNR} = 20 \log_{10} \left(\frac{I_{\max}}{\sqrt{\text{MSE}}} \right) \tag{5}$$

where $I_{\max}$ is the maximum signal value of the input image (I) data type. For example, if the input image has a double-precision floating point data type, then $I_{\max} = 1$, else if it has an 8-bit unsigned integer data type, $I_{\max} = 255$. The lower the PSNR value, the larger the distortion between the original and the watermarked image.

B. NPCR and UACI Analysis

Number of Pixel Change Rate (NPCR) means the percentage difference of pixels among the original image and the encrypted image. The NPCR can be defined mathematically as [21];

$$\text{NPCR} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j)}{M \times N} \times 100, \tag{6}$$

$$D(i,j) = \begin{cases} 0, & \text{if } C1(i,j) = C2(i,j) \\ 1, & \text{if } C1(i,j) \neq C2(i,j) \end{cases} \tag{7}$$

Let $C1(i,j)$ be the pixel values of the one image (original, encrypted or watermarked) and $C2(i,j)$, another image (original, encrypted or watermarked) in the two experiments conducted at the i^{th} pixel row M and j^{th} column N. The value of NPCR shows the degree to which the pixels have been randomly changed. Therefore, the higher the value, the more the change in pixel locations and vice versa.

The Unified Average Changing Intensity (UACI) is the average intensity of difference in pixels. The UACI can also be defined mathematically as [4];

$$\text{UACI} = \frac{1}{M \times N}\left[\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C1(i,j) - C2(i,j)}{255}\right] \times 100 \quad (8)$$

The UACI values from Table 1 depicts that most of the pixel values of the encrypted image have been changed as compared to the original image and vice versa on one hand and that for the watermarked image and the original shows a minimal change.

Table 1 depicts the analysis of the proposed algorithm based on the MSE, PSNR, NPCR and UACI metrics. The higher value of MSE recorded in the Original & Encrypted image shows the larger difference between the original image and the encrypted while the lower value of MSE recorded in the Original & Watermarked image also shows the similarities between the original image and the watermarked image. On the other hand, the lower value of PSNR recorded in the Original & Encrypted indicates larger visual distortion between the original and the encrypted image, whiles the higher values of PSNR in the Original & Watermarked image show how negligible the distortion between the Original and Watermarked image is.

The high measure recorded for the NPCR in Original & Encrypted indicates that the majority of the pixel positions have been randomly changed while that of the Original & Watermarked shows that, just a few of the pixels have been changed. The lower UACI value in the Original & Encrypted image also depicts the higher change in pixel intensity of the encrypted image as compared to the original image while the higher value of the Original & Watermarked image shows minimal change in pixel intensity as compared to the original. This makes it difficult to associate the encrypted image to the original image which could provide clues for attackers. On the other hand, attackers are not able to identify that there is a hidden image in the "watermarked Lena" image since there is no much distortion in the watermarked image.

4.3. Statistical Analysis

The statistical analysis of an encrypted or watermarked image provides much information about the security of the image.

A. Histogram Analysis

An encrypted image is secured against attacks if its histogram is entirely different from the histogram of its original image. Thus, the two images do not contain statistical similarities [22]. An analysis of the results from Figure 5 reveal that the histogram of the encrypted image is totally different from the histogram

Table 1. PSNR, MSE, NPCR AND UACI comparison.

Image	PSNR	MSE	NPCR (%)	UACI (%)
Original & Encrypted	13.66	36.55	99.6680	19.1495
Original & Watermarked	48.87	0.978	13.5481	32.6742

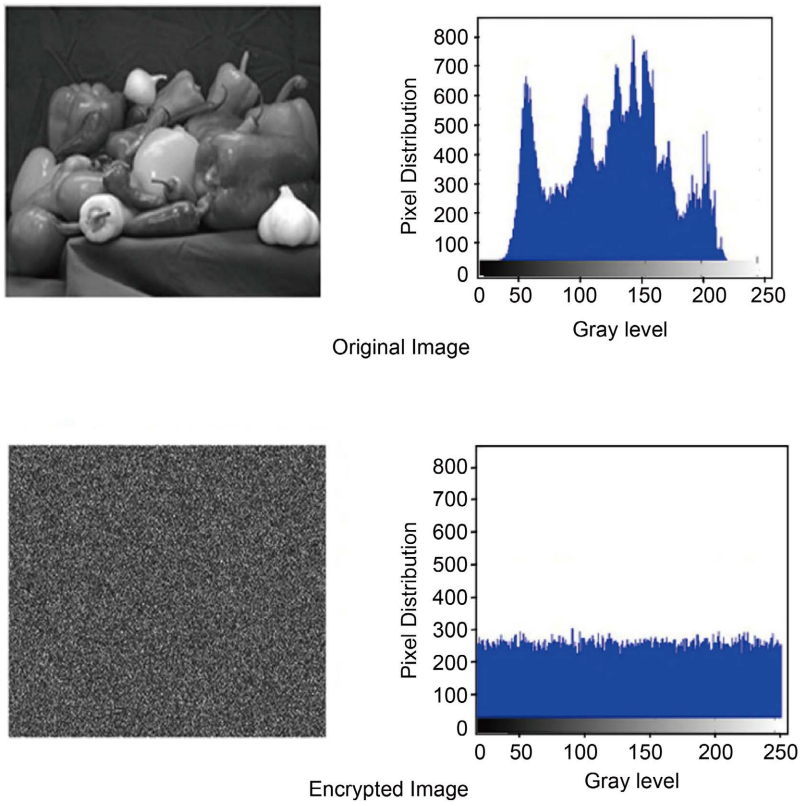

Figure 5. Histogram of original and encrypted images.

of its original image. It does not contain any statistical similarities that may provide any clue about its original image. Therefore, the proposed scheme is secure against histogram attacks.

Figure 5 shows the histogram of the original image and the encrypted image. The histogram of the original image contains large sharp rises and declines whiles the histogram of the encrypted image shows uniform distribution making them differ significantly from each other and has no statistical similarities.

Figure 6 shows the histogram of the original and watermarked images. It can be seen clearly that, both histograms possesses statistical similarities making it difficult for an attacker to detect that there is an embedded image.

4.4. Speed Test

The speed test is a measure of the time taken to execute the proposed scheme. How complex the scheme is, is determine by its execution time. Table 2 shows the time taken (in seconds) for encrypting and embedding the encrypted image and the extraction and decryption of the encrypted image. The execution time of the algorithm from the table shows optimal performance.

4.5. Performance Evaluation

The performance of the scheme is compared with existing schemes by [23] whose work utilised nonlinear spatiotemporal chaotic map and integer wavelet

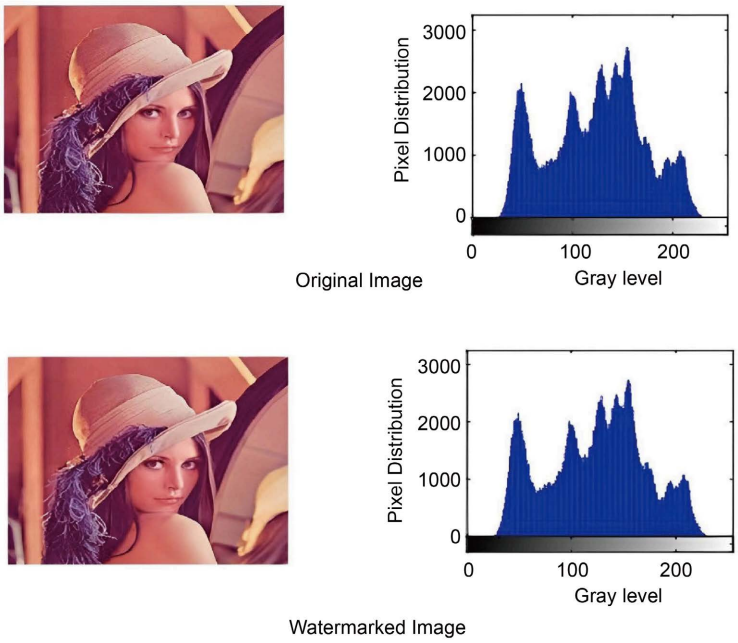

Figure 6. Histogram of original and watermarked images.

Table 2. Encrypted vs. watermarked: MSE and PSNR comparison.

Image	Scheme	MSE	PSNR	Time
Encrypted Image	[23]	8.8315	8509.9886	NA
	Proposed	18.7325	8610.5236	0.06579
Watermarked Image	[24]	48.23	0.0976	NA
	Proposed	62.48	0.657	0.01257

transform (IWT) to encrypt an image. The proposed scheme was also compared with the existing scheme by [24] which, also employed DWT to perform image watermarking. Table 2 depicts the level of noise or changes introduced into the encrypted images. The values for the encrypted image in the table indicates that, there is much distortion in the proposed scheme as compared to the existing scheme whiles that of the watermarked image indicates that minimal distortion exists in the watermarked image of the proposed scheme as compared to the existing scheme.

Table 3 also compares the NPCR and UACI values of the proposed scheme with the existing scheme by [25] whose work focused on the use of hash function with two-round diffusion process to encrypt an image whiles The NPCR and UACI values of the proposed scheme on the watermarked image was also compared with the existing scheme by [26]. The existing scheme leveraged on non sub-sampled contourlet transform (NSCT), redundant discrete wavelet transform (RDWT) and singular value decomposition (SVD) approach. The results indicates that the proposed scheme performed favourably better as compared to the existing schemes.

Table 3. Encrypted vs. watermarked: NPCR and UACI comparison.

Image	Scheme	MSE	PSNR
Encrypted Image	[25]	99.6628	33.6510
	Proposed	99.6680	33.6537
Watermarked Image	[26]	0.9961	0.2853
	Proposed	0.9882	0.2869

5. Conclusion

Privacy in this era of technological dispensation has become a challenge in the film and TV industry. In this paper, a new digital watermarking scheme using GA and Residual Numbers (GARN) was proposed. The results of the simulation show that the proposed scheme is imperceptible and robust.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Yu, X.Y., Wang, C.Y. and Zhou, X. (2018) A Survey on Robust Video Watermarking Algorithms for Copyright Protection. *Applied Sciences*, **8**, Article 1891. https://doi.org/10.3390/app8101891

[2] Bertini, F., Rizzo, S.G. and Montesi, D. (2019) Can Information Hiding in Social Media Posts Represent a Threat? *IEEE Computer*, **52**, 52-60. https://doi.org/10.1109/MC.2019.2917199

[3] Khanzadi, H., Eshghi, M. and Borujeni, S.E. (2014) Image Encryption Using Random Bit Sequence Based on Chaotic Maps. *Arabian Journal for Science and Engineering*, **39**, 1039-1047. https://doi.org/10.1007/s13369-013-0713-z

[4] Verma, V.S. and Jha, R.K. (2015) An Overview of Robust Digital Image Watermarking. *IETE Technical Review*, **32**, 479-496. https://doi.org/10.1080/02564602.2015.1042927

[5] Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G.K.D., Ravi, R.V. and Manikandababu, C.S. (2020) Digital Watermarking Techniques for Image Security: A Review. *Journal of Ambient Intelligence and Humanized Computing*, **11**, 3221-3229. https://doi.org/10.1007/s12652-019-01500-1

[6] Averkiou, M. (2015) Digital Watermarking. Department of Computer Science University of Cyprus. https://api.semanticscholar.org/CorpusID:5553428

[7] Al Embaby, A., Wahby Shalaby, M.A. and Elsayed, K.M. (2020) Digital Watermarking Properties, Classification and Techniques. *International Journal of Engineering and Advanced Technology*, **9**, 2742-2750. https://doi.org/10.35940/ijeat.C5773.029320

[8] Baagyere, E.Y., Agbedemnab, P.A., Qin, Z., Daabo, M.I. and Qin, Z.G. (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

[9] Yang, J.H., Chang, C.C. and Chen, C.Y. (2004) A High-Speed Division Algorithm in

Residue Number System Using Parity-Checking Technique. *International Journal of Computer Mathematics*, **81**, 775-780. https://doi.org/10.1080/00207160410001708805

[10] Agbedemnab, P.A.N., Baagyere, E.Y. and Daabo, M.I. (2019) A Novel Text Encryption and Decryption Scheme Using the Genetic Algorithm and Residual Numbers. *Kalpa Publications in Computing*, **12**, 20-31.

[11] Ram, B. (2013) Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform. *International Journal of Science and Research*, **10**, 1257-1264.

[12] Debnath, L. and Shah, F.A. (2017) Lecture Notes on Wavelet Transforms. Birkhäuser, Cham. https://doi.org/10.1007/978-3-319-59433-0

[13] El Houby, E.M.F. and Yassin, N.I.R. (2020) Wavelet-Hadamard Based Blind Image Watermarking Using Genetic Algorithm and Decision Tree. *Multimedia Tools and Applications*, **79**, 28453-28474. https://doi.org/10.1007/s11042-020-09333-3

[14] Mood, N.N. and Konkula, V.S. (2018) A Novel Image Watermarking Scheme Based on Wavelet Transform and Genetic Algorithm. *International Journal of Intelligent Engineering and Systems*, **11**, 251-260. https://doi.org/10.22266/ijies2018.0630.27

[15] Prakasa Rao, R.S. and Kumar, P.R. (2017) Digital Signature Based Image Watermarking Using GA and PSO. *International Journal of Engineering Research & Technology*, **6**, 373-380. https://doi.org/10.17577/IJERTV6IS060208

[16] Singh, M. and Saxena, A. (2017) Image Watermarking Using Discrete Cosine Transform [DCT] and Genetic Algorithm [GA]. *International Journal of Innovation in Engineering Research & Management*, **4**, 1-13.

[17] Singh, S.K., Gopi, V.P. and Palanisamy, P. (2014) Image Security Using DES and RNS with Reversible Watermarking. 2014 *International Conference on Electronics and Communication Systems* (*ICECS*), Coimbatore, 13-14 February 2014, 1-5.

[18] Banerjee, S., Chakraborty, S., Dey, N., Pal, A.K. and Ray, R. (2015) High Payload Watermarking Using Residue Number System. *International Journal of Image, Graphics and Signal Processing*, **7**, 1-8. https://doi.org/10.5815/ijigsp.2015.03.01

[19] Bhangale, P.P., Gawad, A., Maurya, J. and Raje, R.S. (2017) Image Security Using AES and RNS with Reversible Watermarking. *International Journal of Innovation Science, Engineering & Technology*, **4**, 350-355.

[20] Maji, S. and Nath, A. (2016) Scope and Issues in α Compositing Technology. *International and Issues in Alpha Compositing Technology*, **2**, 38-43.

[21] Özkaynak, F. (2017) Role of NPCR and UACI Tests in Security Problems of Chaos Based Image Encryption Algorithms and Possible Solution Proposals. 2017 *International Conference on Computer Science and Engineering* (*UBMK*), Antalya, 5-8 October 2017, 621-624. https://doi.org/10.1109/UBMK.2017.8093481

[22] Jolfaei, A. and Mirghadri, A. (2010) An Image Encryption Approach Using Chaos and Stream Cipher. *Journal of Theoretical and Applied Information Technology*, **19**, 117-125.

[23] Loukhaoukha, K., Chouinard, J.Y. and Berdai, A. (2012) A Secure Image Encryption Algorithm Based on Rubik's Cube Principle. *Journal of Electrical and Computer Engineering*, **2012**, Article ID: 173931. https://doi.org/10.1155/2012/173931

[24] Sharma, P. and Swami, S. (2013) Digital Image Watermarking Using 3 Level Discrete Wavelet Transform. *Conference on Advances in Communication and Control Systems* (*CAC2S* 2013), 129-133. https://www.atlantis-press.com/article/6291

[25] Norouzi, B., Seyedzadeh, S.M., Mirzakuchaki, S. and Mosavi, M.R. (2014) A Novel

Image Encryption Based on Hash Function with Only Two-Round Diffusion Process. *Multimedia Systems*, **20**, 45-64. https://doi.org/10.1007/s00530-013-0314-4

[26] Thakur, S., Singh, A.K., Ghrera, S.P. and Mohan, A. (2020) Chaotic Based Secure Watermarking Approach for Medical Images. *Multimedia Tools and Applications*, **79**, 4263-4276. https://doi.org/10.1007/s11042-018-6691-0