INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN MULTIDISCIPLINARY STUDIES
(IJARMS), VOL. 2, NO. 1, JUNE, 2022 ISSN 2756-4444
E-ISSN 2756-4452

ENHANCING IMAGE SECURITY USING DATA ENCRYPTION STANDARD, DISCRETE WAVELET TRANFROM WATERMARKING RESIDUE NUMBER SYSTEM AND GAUSSIAN FILTERING

BY

Bolaji Asaju: Department of Computer Science, Faculty of Information and Communication Technology,
Kwara State University, Malete

Damilola David Popoola: Department of Computer Science, Faculty of Information and Communication Technology, Kwara State University, Malete
&
Professor Kazeem Alagbe Gbolagade: Department of Computer Science, Faculty of Information and Communication Technology, Kwara State University, Malete

Abstract
Image encryption is the process of transforming images for its security. The security of digital images has attracted more attention recently due to the need to send images without fear of being attacked. Different schemes have been used to address security problems such as Data Encryption Standard (DES) using Residue Number System (RNS) and Advanced Encryption Standard (AES) using RNS. However, the former has a blurry result. Therefore, this study presents the enhancement of image security using Data Encryption Standard, Discrete Wavelet Transform Watermarking, Residue Number System and Gaussian Filtering. The developed system utilized RNS on a reversible watermarked image using Discrete Wavelet Transform (DWT) and encrypted using Data Encryption key. The encrypted images was converted to RNS with the moduli set {2^{n+1} -1, 2n, 2n-1} this process completes the encryption stage. The decryption was done using the Chinese Remainder Theorem and the cipher key was provided for DES decryption, which also performs reversible watermarking. .
Keywords: Image encryption, Data encryption, Residue number system and Reversible watermarking

Introduction

Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Encryption is the process of transforming the information for its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private (Radhadevi & Kalpana, 2017)**.** Traditional image encryption algorithm such as data encryption standard (DES), has the weakness of low-level efficiency when the image is large. As a result, different security techniques have been used to provide the required protection (Brindha, *et al*, 2015). The security of digital images has become more and more important due to the rapid evolution of the internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images (Nentawe & Goshwe, 2016). Image encryption techniques try to convert an image to another one that is hard to understand (Brindha *et al*, 2015). On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. There are two major groups of image encryption algorithms: (a) Non-chaos selective methods and (b) Chaos-based selective or non-selective methods (Gary, 2016). Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption (Mayank *et al*, 2015).

Encryption of image is really essential in areas such as confidential transmissions, video surveillance, law enforcement, military operations and medical sciences in order to ensure its authorized access. Encryption refers to encoding of image with some algorithm while decryption is decoding the image with reverse steps. Image encryption not only prevents the encrypted image from being intercepted but also ensures that image can only be decrypted, interpreted and viewed by the intended person. In Digital watermarking, an imperceptible signal referred as a watermark is embedded into multimedia data for various purposes such as copyright protection, fingerprinting, authentication, etc. The embedding of the watermark usually

introduces irreversible distortion, although it may be quite small, in the original data. For applications where the availability of original data is essential, irreversible degradation of the original data is not acceptable, and incurred distortions need to be removed. Examples of such applications include multimedia archives, military image processing, and medical image processing for electronic patient records (EPRs) (Radhadevi & Kalpana, 2017). In multimedia archives, a content provider may not want the original content to be distorted even though the distortion is imperceptible to most users, and it may be too costly in terms of storage space to store both the original and the watermarked versions in military image processing, images are gathered at a very high cost and are usually subjected to further processing steps such as extreme magnification. Any distortion may hinder accurate analysis of the image. Reversible watermarking is data embedding, which is also called as lossless data embedding, embeds data called payload such as image or data in a fashion so that the original image and the payload is recovered without any losses.

Residue Number System (RNS) is defined by a set of number (m_l, m_2, ... m_k) called moduli, which are relatively prime to each other, i.e. two moduli should not have a greatest common divisor greater than 1. Hence, each integer number X can be mapped onto the legitimate range and represented as an N-tuple of residue digits (R_1, R_2, ... , R_n). Data Conversion in residue number system is usually based on either the Chinese Remainder Theorem (CRT)] or the Mixed Radix Conversion (MRC), which can be categorized into forward and reverse conversions (Popoola, 2019)
DES is an implementation of a Feistel Cipher. The block size is 64bit. It has a limited key size of 56 bits thus only 2^56 keys are possible (Brindha *et al*, 2015). These keys can be determined easily. Hardware implementations of DES are very fast. It was not designed for software, so runs relatively slower for software. This research work helps to enhance image security using Data Encryption Standard (DES) using Residue Number System (RNS) on Discrete Wavelet Transform (DWT) watermarked images, this combination helps to overcomes the individual drawbacks of each one and provides a more secure watermark which is difficult for the intruder to extract using RNS forward and reverse conversion.

Images are the most important utility of our life, they are used in many applications. The level of importance attached to an image made it inevitable to provide a mechanism to protect images sent over a network against any form of attack or access by a third party. During the past years several image encryption and authentication algorithms have been proposed and has equally attained good results. Nevertheless, these algorithms have some problems which will render the image useless, making it ineffective for the purpose this is meant for. In an attempt to improve on the existing schemes, DES algorithm was proposed to be used to encrypt image and has proven to be fast and achieve good image encryption rate. Although the scheme was effective, the resulting image was blurry thereby making the image lack the required originality. To improve on this, a scheme was proposed using AES algorithm, this produced a clean image but in a white and black format. Therefore, a scheme was proposed to improve the performance of existing schemes by producing a coloured image while maintaining its originality through the use of Gaussian filter and further increase level of security.

Literature Review
Today, various people utilize the distinctive applications to image data transfer. By far most of the people use their images for various customers using the social application. The attack on these social applications can copy or hack the important data. For better usage of these applications, users are using it on their mobiles, tablets, etc. The protection against the hacking attacks on those web or available is plans, there exist distinctive data security framework for multimedia data. These present security frameworks are either using encryption or steganography, or the combination of both. There is diverse securable image encryption that can be especially for protection against the unauthorized access. A transferred over the internet having important data of military, security associations, social or adaptable applications. Hence the image security is necessary. The commonly used security mechanisms are DFT, DCT and DWT (Totla & Bapat, 2017). The transfer of the image over the unsecured network will pose following attacks such as active and passive attacks. Active attacks: This consists of few data stream modification or false data stream creation. Passive attacks: This attack uses the data but not affect the system resources.

Methodology
The process is of two major phases; image enrollment and authentication stage. During the enrollment stage, the supplied image is loaded to the platform, followed by the pre-processing stage which include the

application of DWT watermarking, which is then passed to the data encryption standard for image encryption. After the image is successfully encrypted, the residual number system is used by applying RNS forward conversion for further encryption of the image, this helps to enhance the image security. The authentication stage involves the reverse process of the enrollment stage, at this stage, the encrypted watermarked image is passed to the RNS backward conversion followed by the DWT watermark this helps to remove the watermark in the image and lastly the DES performs the decryption with the correct cipher key.

In this process, firstly our original image (host image) is taken and 2D, 3- level DWT is applied to the image which decomposes image into low frequency and high frequency components. The technique used here for inserting the watermark is the alpha blending which embeds visible/invisible watermark into salient features of original image

The decomposed components of the original image and watermark are multiplied by a scaling factor and added. Since the watermark embedded into this work is visible, it is embedded in low frequency approximation component of the original image. According to the formula of the alpha blending, the watermarked image is given by bands

LL2, LH2, HL2 and HH2

WM1=k * (LL2) + q* (WM2)

Where WMI = Low frequency component of the watermarked images, LL3= low frequency component of the original image by 3 – level DWT, WM3= low frequency of watermark image, and K, qz scaling factors for the original image and watermark respectively.

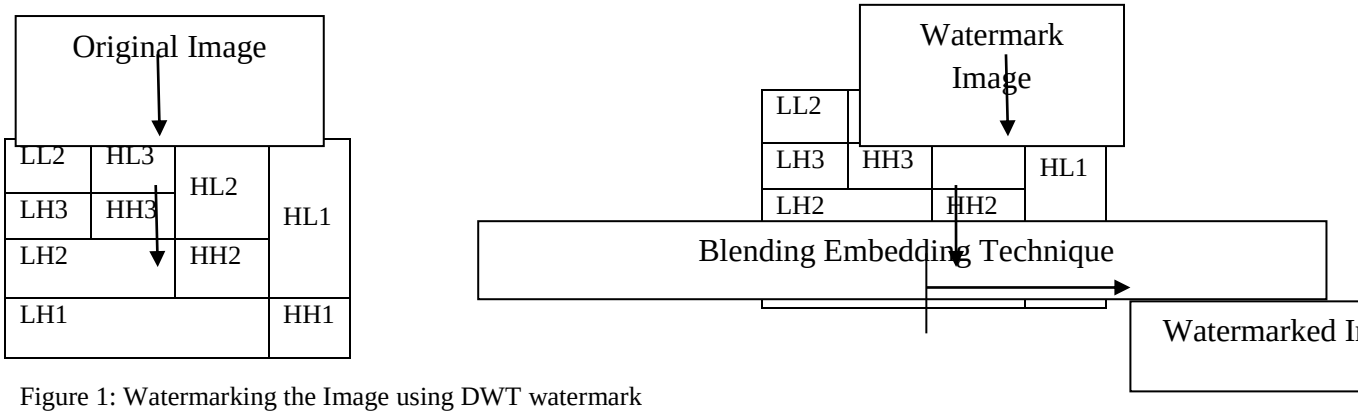

Figure 1: Watermarking the Image using DWT watermark

In other words, an image is hidden in the original image to give a different picture from the original image.

Image loading

Sample images are taken randomly from domain expert to evaluate the developed system. The images are loaded at random into the graphical user interface. A total of 10 images was sampled for experimental purpose.

DES Encryption and decryption

The Stepwise method for the implementation of the BLOWFISH, DES and AES algorithm for the encryption and decryption of data is explicitly stated thus;

DES Algorithm

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.
2. The plaintext block has to shift the bits around.
3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4. The plaintext and key will processed by following.

a. The key is split into two 28 halves
b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
c. The halves are recombined and subject to a compression permutation to reduce the key from 56bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
d. The rotated key halves from step 2 are used in next round.
e. The data block is split into two 32-bit halves.

f. One half is subject to an expansion permutation to increase its size to 48 bits.
g. Output of step 6 is exclusive-OR'ed with the 48-bit compressed key from step 3.
h. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
i. Output of step 8 is subject to a P-box to permute the bits.
j. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

Results and Discussions

The developed system emphasized the effect of Residual Number System on a reversible water marked image using Discrete Wavelet Transform and Data Encryption Standard for first stage image security. The system was experimented upon with samples of Nigerian Car Plate numbers collected. The image was watermarked with a chosen image from the DWT watermark bank to hide the content of the image before encryption. The watermarking was carried out by the discrete wavelet transform algorithm, the result of watermarked image was passed to the Data Encryption Algorithm (DES), the DES algorithm performs a first stage of encryption using the supplied key cipher, the encrypted image is passed to the Residual Number System with the moduli set of $m_1 = 2^{n+1} - 1, m_2 = 2^n$ *and* $m_3 = 2^n - 1$. The forward conversion process was used to further encrypt the image which was spitted into three residues. This process completes the encryption stage, the decryption stage was initiated by supplying the moduli set that was used to the forward for the process of reverse conversion, the reverse conversion is used to decrypt the image which combines the three residues to singular image producing the decrypted image, after which the DES decryption is triggered with the same cipher key used for encryption is supplied which brings the inverse of the watermark image or which performs the reversible watermark to bring out the image that was watermarked with the Gaussian Filtering Completing the process. The experiment also reveals that the filtered imaged helps to contribute to faster computational time as compared to the non-filtered image which occurs after the decryption of the encrypted image.

Interactive Developmental Stage

The over-all developed system is shown below. The GUI screen is the onload screen when the application is initiated with eight major axes for image operations for loading, and showing the encryption/decryption result.

Experimental Data and Software Testing

Figure 2 shows when an input image is loaded into the system. The original image is loaded as well as the watermark image to be processed with the original image for concealing.

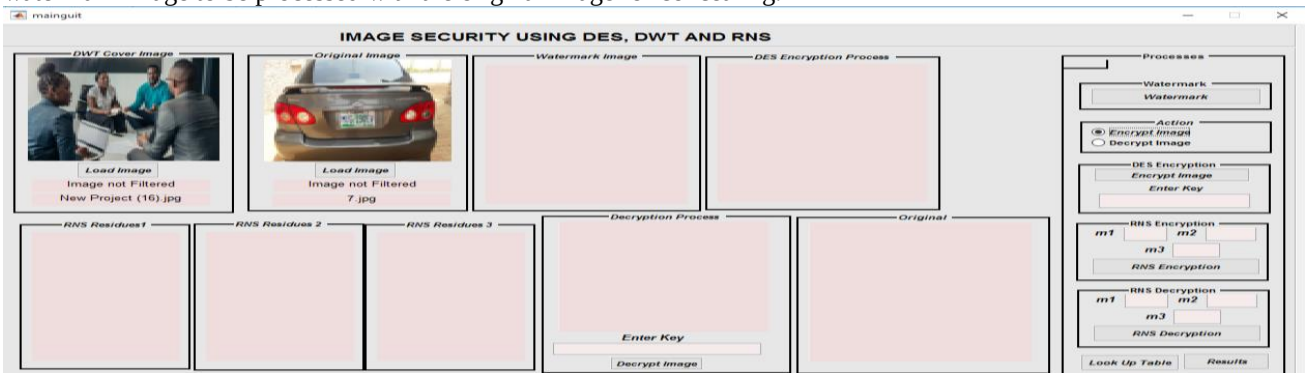

Figure 2: loading of input images.

DWT Watermarking

Figure 3 shows the image after watermarking processing btw the discrete wavelength transform algorithm, it returns a single output image after concealing the watermark image in the original image.

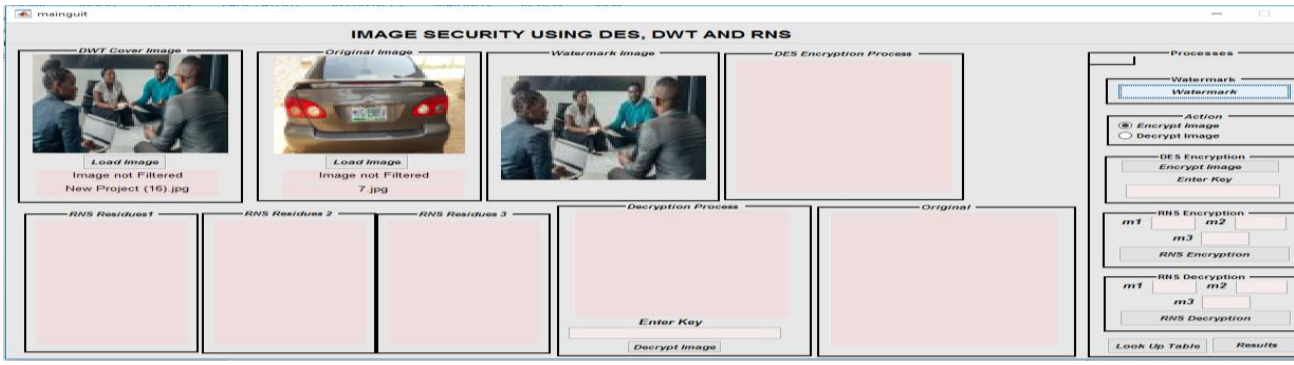

Figure 3: DWT Watermarking

Data Standard Encryption (DES)

Figure 4 shows the image when it is encrypted by the Data Standard Encryption Algorithm after the supply of a cipher key which is converted and simulated to a 64 byte key size to perform the encryption of the already watermarked image.

Figure 3: Block truncate Compression Process

Residual Number System Second Level Encryption Stage (RNS)

The result of the second stage encryption by the RNS forward conversion process the moduli set of 7, 4 and 3. The RNS takes the pixel value of the encrypted watermarked as input and finds the residue of those pixel value which is spited into three image residues for m1, m2 and m3 taking$m_1 = 2^{n+1} - 1, m_2 = 2^n$ *and* $m_3 = 2^n - 1$ and the value of n to be 2.

Residual Number System Decryption Stage Reverse Conversion (RNS)

The result of RNS after the reverse conversion which converts the image pixel to the initial or original image pixel value after the DES decryption value using the Chinese remainder theorem. The correct moduli set of 7, 4, and 3 must be supplied to reverse the image back. The results brings back the image Encrypted by the DES algorithm.

DES Decryption

After successful execution of the RNS reverse conversionthe DES Encrypted image was returned which was processed with the same cipher key that was used for encryption the correct entry of the cipher key prompts the decryption of the image as well as the reversible watermark image which returns the original image before it was watermarked.

Filtered Output

The interface below shows final results of the system process as the result obtained after successful decryption of the images which gives a better output by reducing noise and blurriness from the decrypted image.

Figure 4: Gaussian Filtering.

Experimental Evaluation

The system was tested over three sample images. The obtained results is shown below for both the filtering and non-filtering case. The tables shows results a t timing and memory level at both encryption and decryption stage.

Encryption and Decryption Results

Table 1: Encryption and Decryption Results

	Timing Results			
Samples	Encryption Time (RNS) secs	Encryption Time (DES) secs	Decryption Time(RNS) secs	Decryption Time (DES) secs
Image Sample 1(Original + Watermark)	3.4004	15.0245	0.0864	0.3130
Image Sample 2(Original + Watermark)	3.7307	15.0220	0.084608	0.32897
Image Sample 3(Original + Watermark)	3.9187	15.0283	0.09489	0.20249
Image Sample 4(Original + Watermark)	3.7374	15.0292	0.14566	0.57353
Average	**3.6968**	**15.026**	**1.03E-01**	**3.54E-01**

The average encryption time shows that the RNS has a faster computational time than the DES algorithm with 3.6968 secs as compared to 15.026 secs. The average Decryption time shows that the RNS has a faster computational decryption time than the DES algorithm with 0.1029 secs as compared to 0.3545 secs. The average encryption memory also shows that the RNS consumes lesser memory space for its computation as compared with the DES algorithm which is measured in decibels. The average decryption memory also shows that the RNS consumes lesser memory space for its computation as compared with the DES algorithm which is measured in decibels.

Comparative Evaluation with Relate Works

Table 2: Comparison with existing work

Work	Average Encryption Time	Average Decryption Time	Level of Security	Layers
Suraj Kumar Singh	19.5668	0.52	Moderate	2
Experimented Results	18.7228	0.45	High	3

Conclusion

For the protection of digital data over internet, security methods are required. So, there are various methods for security of data over internet. But the combination of cryptography and watermark is more secure cryptography and watermark provides security and authentication to the secret image. This project also enhances the image security with RNS as sometimes, DES can be opened to brute force attack. The developed model of image security requires secret key and RNS moduli set to recover the original image after watermarking takes place. The watermarking process was able to provide an initial stage of image security by hiding or watermarking the image inside another image which even made the image ambiguous to a neutral user. The system was tested and examined based on the computational time and memory space used to run each of the algorithm considered.

Recommendations

It is recommended that

1. Other encryption techniques like the asymmetric or elliptical cryptographic method be combined with RNS to further enhance the security especially when the usability of such system is deployed in the cloud or internet for use.
2. Other reverse conversion methods such as Mixed Radix Conversion (MRC) and New Chinese Remainder Theorem (N-CRT) should adopted in order to measure the efficiency of the traditional CRT.
3. This method should be adopted on moving images and videos.

References

Ayushi, R. (2017). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications.* 1(15), 0975 – 8887.

Brindha, K, Sharma, R & Saini, S. (2015). Use of Symmetric Algorithm for Image Encryption, *International Journal of Innovative Research in Computer and Communication Engineering,* 2(1), 4401- 4407.

Gary, C. (2016). An Overview of Cryptography: Cryptographic, HLAN, ver. 1,1999-2016.

Mayank, D., Singh, P & Garg, C. (2015). A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping *International Journal of Information & Computation Technology*. 4(7), 741-746.

Nentawe, R & Goshwe, Y. (2016). Data Encryption and Decryption Using RSA Algorithm in a Network Environment. *International Journal of Computer Science and Network Security*, 13(7), 9-13.

Popoola, D. D. (2019). Data integrity using caesar cipher and residue number system (13897657). Available from Dissertations & Theses @ Kwara State University. (2248761367). Retrieved from https://search.proquest.com/docview/2248761367?accountid=171549

Radhadevi, P & Kalpana, P. (2017) Secure Image Encryption Using AES, International Journal of Research in Engineering and Technology, 1(2), 115-117.

Totla R.V & Bapat K.S. (2017). Comparative Analysis of Watermarking in Digital Images using DCT and DWT, *International Journal of Scientific and Research Publications.* 3(2), 1-4.