JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(2), JUNE, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

Development of an Improved Steganography-based Patient Management Information System

Idakwo M. A.
Department of Computer Engineering,
Ahmadu Bello University, Zaria Kaduna State, Nigeria.

ABSTRACT
This paper developed an improved patient management information system with covert communication. The developed system covertly communicates (steganography) patient's sensitive information (payload) using digital images over the Intranet/Internet without arousing suspicion, distorting the image quality (imperceptibility), or modifying the information (robustness to attacks).To avoid truncation of information during the embedding of information in the patient's digital images, a novel real-time redundant bit evaluator was developed. Upon a successful brute force on the system, a secure self-destructive scheme was developed to securely remove all the embedded sensitive information from the digital images (referred to as stego-images). The evaluation of the secure self-destructive scheme was performed on a developed user-friendly Adaptive Integer Diamond (AID) simulator in MATLAB 2020a using the cover-image and the generated stego-image. The peak signal-to-noise ratio (PSNR), structural similarity index (SSIM) and mean square error (MSE) obtained from the evaluation are infinity, 1.00, and 0.000 respectively. This indicates that both the cover-image and stego-image are identical, thus the stego-image contains no sensitive information. The developed system is robust to single and hybrid attacks such as compression, Gaussian noise, salt and pepper, rotation, salt and pepper with Gaussian noise, cropping, and rotation, with an average improvement of 64.71%, 81.67%, 57.63%, 46.70%, 83.50%, and 64.83% respectively over state of the art.

ARTICLE INFO
Article History
Received: March, 2022
Received in revised form: March, 2022
Accepted: March, 2022
Published online: May, 2022

KEYWORDS
Cover-image, Patient Management information system, imperceptibility, steganography, Stego-image, Stego-keys.

.

INTRODUCTION

Guarantying sensitive information privacy is vital in communication [1]. The health sector where privacy and confidentiality of information are paramount for instance [3], shares data accruing from outbreak investigations, public health-oriented research, and diversity of medical information systems, and likewise refer patients to other health institutions using public networks [2]. These health or medical information are comprehensive records consisting of medical histories, drug information, and discharge histories of an individual or patient health [4]. This information is very sensitive and if inappropriately shared or misused can distress, embarrass, and cause financial loss, death, or other damages to patients thus, the essence of the varying laws ranging from state, federal, licensure, certification laws, and Hippocratic oath [5] on doctors' general duty of confidentiality [6]. The persistence problem inherently in paper documentation drifted for the recommendation and adoption of a patient management information system (PMIS) [7]. Furthermore, the pursuit to improve organizational efficiency, increase patient safety, lower medical errors, lower duplication of services, optimize reimbursement, and compete locally and globally has since then motivated the continual integration of information technology in the health sector [8]. Nonetheless, the stringent privacy and confidentiality requirement on patient information made it expedient to devise strategies for securing patient information during storage and

Corresponding author: Idakwo, M.A. ✉ mondabutuj@gmail.com ✉ Department of Computer Engineering, Ahmadu Bello University, Zaria.

exchange [9] to evade privacy and confidentiality violation. Information security breaches do not only affect individuals but significantly affect organizational reputation [10]. Therefore, ensuring secure information storage and communication over the intranet/internet has become an important area of focus [11]. As a means of securing health information databases and equally the communicated health information, the cryptographic approach was earlier adopted to obscure the health information into an unintelligent and unreadable form known as ciphertext [12] . These ciphertexts can only be reconstituted by a valid cryptographic key and therefore provided security for the database while maintaining the confidentiality of exchanged medical health information [1]. Nonetheless, transmitting an encrypted image over the public networks attracts the attention of eavesdroppers known as cryptanalysts [15]. Hence, the need for concealing the existence of the communication medium in other to evade eavesdropper attention using steganography [20]. This adoption of steganographic techniques is due to its ability in concealing confidential data within other seemingly innocuous cover-media such as text, video, audio, and images [19]. Steganography has evolved from the simple hiding of confidential information inside the least significant bits of a cover medium to more sophisticated schemes that utilize the transform domain due to obvious advantages related to robustness and imperceptibility. The salient issues in steganography that have spanned over the years are on how to optimally utilize the cover medium redundancy bits especially if a large volume of information needs to be communicated amidst limited redundancy bits while maintaining imperceptibility, robustness and computational time [21]. The adverse effect of perceptibility has relatively reduced the embedding capacity thus leading to a tradeoff between imperceptibility and payload [2]. Interestingly, while the spatial domain guarantees a high payload, the transform domain satisfies imperceptibility and robustness at the expense of higher computational complexity. Therefore, this paper adopted our previously developed non-separable integer-to-integer wavelet transform [1] to develop an improved patient management information system with higher payload, lower imperceptibility, and lower computational complexity. The steganography-based management information system was developed using hypertext preprocessor (PHP) [23], asynchronous JavaScript and extensible makeup language (AJAX) [24], and cascading style sheets (CSS) [25]. The developed system is accessed using the user's browser. The MatLab 2020[26] was used to develop a simulator to evaluate the system performance with the existing system

These paper contributions are highlighted as follows.

1. Development of a real-time redundant bit evaluator counter for controlling embeddable secret information
2. Development of a secure stego-image self-destructive scheme to mitigate steganalyst random guess attack or brute force attack.
3. Development of an unpredictable random number generator for stego-keys
4. evaluate the developed system's robustness to single, hybrids attacks (salt and pepper noise, compression, Gaussian noise, cropping, and rotation),

BACKGROUND OF THE STUDY

Several researchers have deployed steganography in telemedicine applications to conceal patients' diagnoses, prescriptions, and medications. Manoj *et al.* [17] implemented a secured and scalable digital health records sharing system. The system focused on the privacy and security in accessing medical records on a hybrid cloud and was divided into two security domains (personal and public domain) based on data access requirements. Where the public domain users were grouped based on professionalism and the personal domain users were grouped as patients and relatives. A multi-based and key policy attribute-based encryption using 128 bits length was adopted to maintain a secure system control in both groups. These keys were encrypted using the RSA encryption standard. The electronic medical file was partitioned and encrypted using the AES encryption method before storing them in the cloud. The encryption time and average response time for an HTTP request for different group sizes of users in public and private domains were measured and the AES encryption time increases with file sizes and thus requires more bandwidth for transmission, access time, and more storage space requirement.

Corresponding author: Idakwo, M.A. ✉ *mondabutuj@gmail.com* ✉ *Department of Computer Engineering, Ahmadu Bello University, Zaria.*

Similarly, Elhoseny *et al.* [16] implemented a secure steganography system for medical data transmission on the internet using a hybrid secured encryption scheme in a two-dimensional discrete wavelet transform. The secured hybrid scheme was the combination of RSA and AES algorithms for encrypting the secret text in the cover-image. The cover-image was decomposed and transformed into sub-bands using the discrete wavelet transform. In the embedding phase, the secret texts were converted into binary bits using ASCII and divided into even and odd parts. The RSA was used in encrypting the even parts using a public key while the AES was used to encrypt the old parts using a public key. The ciphertext was compressed to reduce its size before embedding it into the cover-image. The private key needed for retrieving the secret text from the stego-image was equally encrypted using AES and securely sent to the receiver. The system concealed the confidential information while maintaining minimal distortion in the stego-image. Although RSA encryption is computationally expensive compared to AES, adopting the two encryption algorithms increased the computation complexity of the system and likewise reduces the cover-image payload. The work of Santoso [17] presented a steganographic system for telemedicine applications. The system was developed to convey confidential medical text information. The cover-image was evaluated using pixel value differencing to search for embeddable regions. The embeddable region is defined by a hiding constant ranging from 3bit to 7 bits and controls the system's imperceptibility. The data embedding priority was solely on high contrast area while fewer bits were embedded in a low contrast area. Nonetheless, the payload of the system is proportional to images with high contrast areas and therefore may not suit all images. Equally, embedding bits based on the defined constant range is not an effective way of evaluating redundant bits as there are high possibilities of over/under utilization of the embedding region which would affect the image quality. To ensure cover-image conveys more sensitive information, Karakus & Avci [14] introduced an optimum pixels similarity for medical images. While the image allows more patient information to be embedded, the perceptibility of the stego-image was not controlled. The work of Ahmad[19] on the other hand used an integer wavelet filter to decompose medical cover-image into a transform domain and adopted arithmetic coding and Data encryption Standard to securely encrypt patient information. This, however, increased the computational complexity of the system. Controlling the perceptibility of patient stego-image has continued to remain a bottleneck neck for researchers due to the high volume of patient data and the unlimited space in the digital image. Thus, deploying steganography to a real-time application to securely convey patient information without any truncation of information while maintaining perceptibility is the bases on which this research is inspired.

IMAGE QUALITATIVE ASSESSMENT

For effective qualitative evaluation of stego-image, structural similarity index, peak signal-to-noise ratio, mean squared error, and histogram are the standard benchmark used with images from University of Granada Computer Vision Group (CVG-UGR) and University of Southern California Signal and Image Processing (USC-SIPI) [28].

Bit error rate

The bit error rate (BER) is used in measuring the ratio between the incorrectly extracted stego-image bits after and before an attack. It is mathematically evaluated using equation (1) [16]:

$$BER = \frac{S_{wa} - S_a}{S_{wa}} \quad (1)$$

Where; S_{wa} are the stego-image bits without any attack.

S_a are the stego-image bits with an attack.

Image histogram

An image histogram is a graphical way of showing the exact pixels distribution and its number of occurrences. The higher the similarity between a cover-image histogram and the corresponding stego-image histogram the smaller the distortion caused by the embedding process [22].

Mean squared error (MSE)

This MSE measures the variability between a stego-image and its cover-image. The closer a mean square error to 0 the higher the

Corresponding author: Idakwo, M.A. ✉ *mondabutuj@gmail.com* ✉ *Department of Computer Engineering, Ahmadu Bello University, Zaria.*

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(2), JUNE, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

accuracy of the system. It is mathematically evaluated using equation (3) [30]:

$$MSE = \frac{1}{\mathrm{m}\,n}\sum_{a=1}^{m}\sum_{b=1}^{n}\left(S_{ab} - C_{ab}\right)^{2} \quad (3)$$

Where; m and n represents the input image rows and columns numbers respectively

S_{ab} and C_{ab} is the stego-image and cover-image respectively

Peak signal-to-noise ratio (PSNR)

The PSNR measures the rate of distortion caused in a stego-image in decibel (dB). The peak signal-to-noise ratio is expressed mathematically using equation (4) [28]:

$$`PSNR = 10\log_{10}\frac{L_{\max}^{2}}{MSE} \quad (4)$$

From equation 4, the cover-image can be defined by a maximum fixed value 255*255, hence the variation of the image is only related to the MSE. The more the information embedded, the larger the MSE. This will result in a lower PSNR which will translate to a higher distortion or lower imperceptibility. On the contrary, smaller embedded information will result in a lower MSE which will increase the PSNR or higher perceptibility [30].

Structural similarity index (SSIM)

The SSIM evaluates the structural similarity between two given images with a ranging value between -1 and 1. An SSIM closer to 1 shows that the given images are nearly the same. The expression given in equation (5) is used to compute the SSIM between a cover-image and the generated stego-image [30].

$$SSIM\left(\mathrm{C}_o,\mathrm{S}_o\right) = \frac{\left(2\mu_{C_o}\mu_{S_o} + k_1\right)\left(2\sigma_{C_oS_o} + k_2\right)}{\left(\mu_{C_o}^2 + \mu_{S_o}^2 + k_1\right)\left(\sigma_{C_o}^2 + \mu_{S_o}^2 + k_2\right)} \quad (5)$$

Where; C_o represents cover image cover

S_o represents the generated stego-image pixels

μ_{C_o}, μ_{S_o} represents cover and stego-pixels mean intensities respectively

$\sigma_{C_o}, \sigma_{S_o}$ is the cover and stego-image variance.

k_{C_o}, k_{S_o} are constants included to avoid instability when $u_{C_o}^2 + u_{S_o}^2$ is very close to zero.

$\mu_{C_o} = u_{S_o} = \left(kL\right)^2$ where L is the dynamic range of the pixel (255 for 8 bit) and k«1

DEVELOPED SYSTEM

The non-separable integer-to-integer wavelet transform and diamond encoding developed in our previous paper [1] was adopted to decompose the patient digital image into diagonal coefficient vertical coefficient, horizontal coefficient, and approximation coefficient. The developed improved patient management information system architecture was designed to suit the sensitive departments (Records, Radiology, Triage, Laboratory, and Medical) which handle patient file movement in the Federal medical center Abuja. The conceptual framework of the developed system is shown in Figure 1. The conceptual framework clearly shows the implementation scenario of the developed system. The system uses the patient's passport as a cover-image to covey each patient's prescription, diagnosis, past medical histories, clinical examinations, and medications.

Corresponding author: Idakwo, M.A. ✉ mondabutuj@gmail.com ✉ Department of Computer Engineering, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(2), JUNE, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

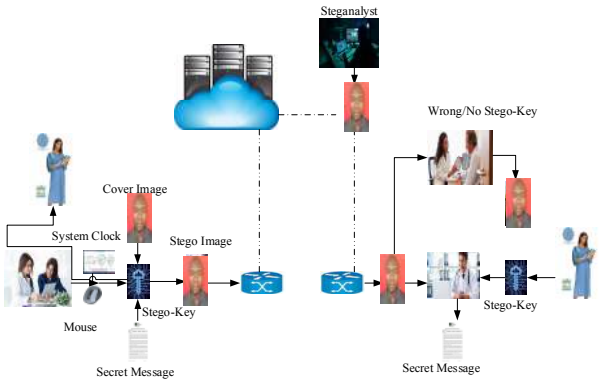


Figure 1: Conceptual Framework of the developed system

Stego-key Generation

The true random numbers generator was developed using PHP, and CSS in a notepad++ text editor. The generator uses the users' computer mouse waiting time and clock. The mouse wait time refers to the total time taken before the developed generator event button is triggered. To evaluate the mouse wait time, it is essential to determine the mouse's position. The CSS was used to determine the mouse current position using the x and y coordinate while AJAX was used for the evaluation of the mouse wait time and equally for fetching the current system date and time. The mouse wait time was evaluated by measuring the serial movement between the coordinates returned from the mouse operation using equation (6):

$$M_t = t_{1x}^{y} - t_{0x}^{y} \quad (6)$$

Where; x refers to the last x-coordinate of the mouse

y is the last y-coordinate of the mouse

t_1 is the final time (milliseconds) spent,

t_0 is the initial start time (ms) at the coordinate position

M_t is the Mouse wait time

To enhance and equally increase the difficulty in reproducing the entropy environment, the mouse wait time was exclusive-OR (XOR) with the system time and calendar using equation (7).

$$s_{dt} XOR m_t = \sum_{k=0}^{[\log_2(s_{dt})]} 2^k \left[\left(\frac{s_{dt}}{2^k} + \frac{m_t}{2^k} \right) \bmod 2 \right] \quad (7)$$

Where; S_{dt} is the system's current DateTime (ms)

The developed generator produced numbers that are expected to be nondeterministic. These numbers are used as stego-keys and are required for both embedding and decoding processes.

Redundant bits Evaluator Counter

The redundant bits evaluator counter (REC) was developed in Ajax using the notepad++ text editor to provide real-time visualization of the embeddable region for the users. The developed steg-patient management information system supports the concealing of either an image or text. However, more priority was given to images in an event where both image and text are the secret information. The flowchart for the developed real-time redundant bit evaluator is shown in Figure 2.

Corresponding author: Idakwo, M.A. ✉ mondabutuj@gmail.com ✉ Department of Computer Engineering, Ahmadu Bello University, Zaria.

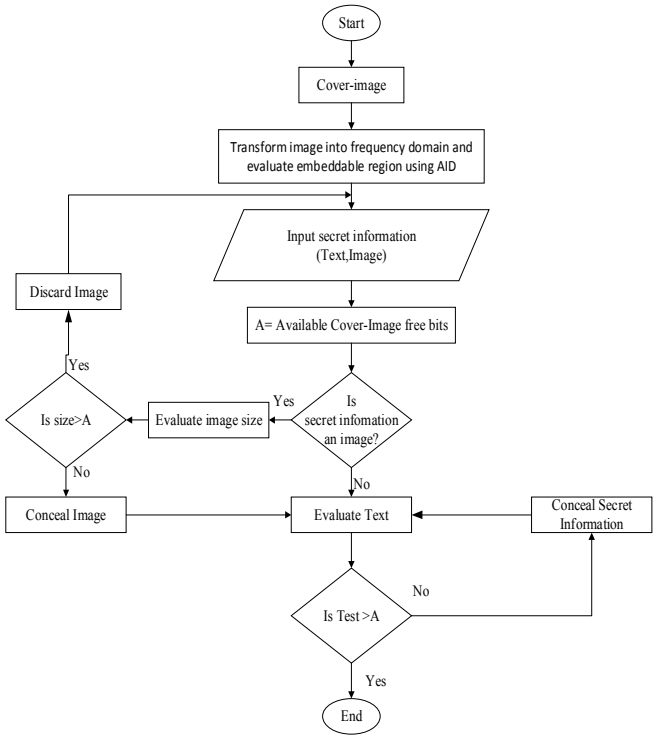


Figure 2: Redundant Bit Evaluator Flowchart

From the flowchart presented in Figure 2, the cover-image is first decomposed into the frequency region, and the image coefficient redundant bits are evaluated using the integrated diamond encoding. The evaluated redundant bits become the embeddable region for the patient information and are display in real-time for the user. If the embedding information contains an image and a text, the secret image size is first evaluated. After the evaluation, the secret image will only be discarded only when the available cover-image redundancy bits cannot accommodate the entire secret image. Otherwise, the secret image is concealed inside the redundancy bits of the cover-image first before embedding the secret text in the remaining redundancy bits. Ajax was responsible for real-time visualization of the remaining bits without interfering or refreshing the display and behaviour of the existing pages.

Stego-image Information Self-Destructive Scheme

To maintain a higher information confidentiality level, a secured stego-image information destructive scheme was developed to mitigate wrong stego-key entries. The developed scheme assumed any wrong stego-key entry is from steganalyst. It was developed in Ajax using the flow chart shown in Figure 3.

Corresponding author: Idakwo, M.A. ✉ mondabutuj@gmail.com ✉ Department of Computer Engineering, Ahmadu Bello University, Zaria.

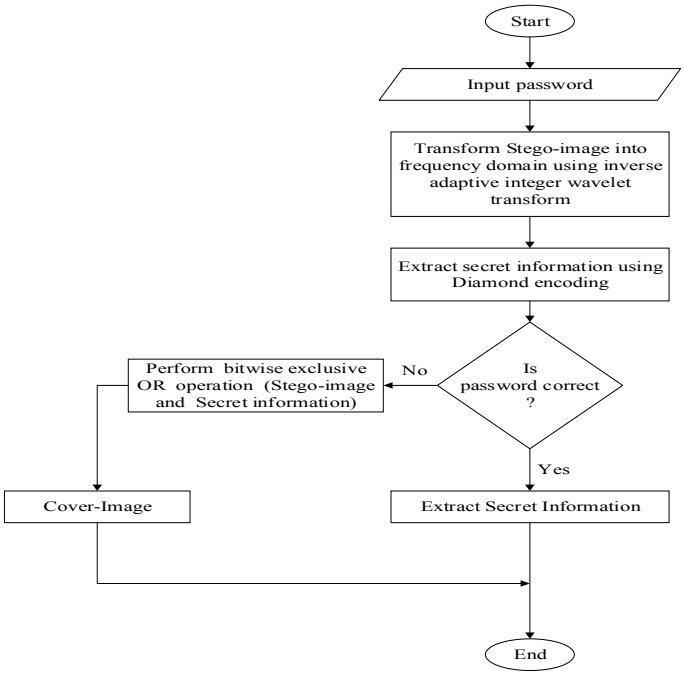


Figure 3: Secure Stego-image Self-Destructive Scheme

From Figure 3, a stego-key is first required for the extraction of the secret information. The user is prompt to provide the required stego-key. Once a key is provided, the stego-image is transformed from the time domain into the frequency domain using the inverse operation of the developed AID technique. The secret information is extracted from the coefficients of the stego image once the secret-key and the embedded key are the same. However, a wrong stego-key provided by the user will trigger a bitwise exclusive OR operation between the stego-image coefficients and secret information. These processes will produce a new coefficient that is different from the stego-image coefficient but the same as the original cover-image coefficient. Thus, the new coefficient will reproduce the initial cover-image coefficient. In a case of a random guess attack, this will fault the guess as the cover-image has no embedded information.

To effectively evaluate the developed system performance with existing system, a user-friendly interface simulator called AID MatLab Simulator as shown in Figure 4, was developed using MatLab 2020 to carry out the analysis .

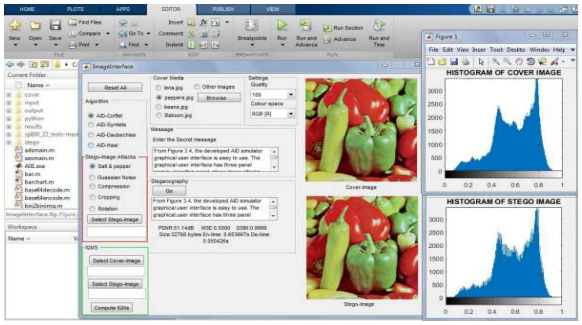


Figure 4: AID Matlab Simulator

Corresponding author: Idakwo, M.A. mondabutuj@gmail.com Department of Computer Engineering, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(2), JUNE, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

RESULTS AND DISCUSSION

Imperceptibility Control

The developed redundant bits evaluator counter provides real-time visualization of the total available bits during the process of concealing patient secret information. This is essential to avoid the truncation of any sensitive information. In other to evaluate the effectiveness of the developed redundant bit evaluator counter the Lena, and pepper images of the same dimension (512 by 512) were selected to covey a patient passport of dimension 450 by 450 and a diagnosis text of 18 bytes using the colour space. The available bits after embedding the patient passport in both images are as presented in Table 1.

Table 1: Available Bits for Secret Text

Image	Available Redundant bits	Embedded bytes
Lena	115	15
Pepper	87	10

From Table 1, it can be observed that images of the same dimensions do not have the same redundant bits. This variation may be due to the light intensity during the image acquisition, noise from the acquisition source, or during file transfer and image contents. Therefore, the real-time redundant bit evaluator counter will help medical practitioners to control their embedding information in patient image. The controlling of the Lena image during the concealing of the patient passport and diagnosis text is shown in Figure 5.

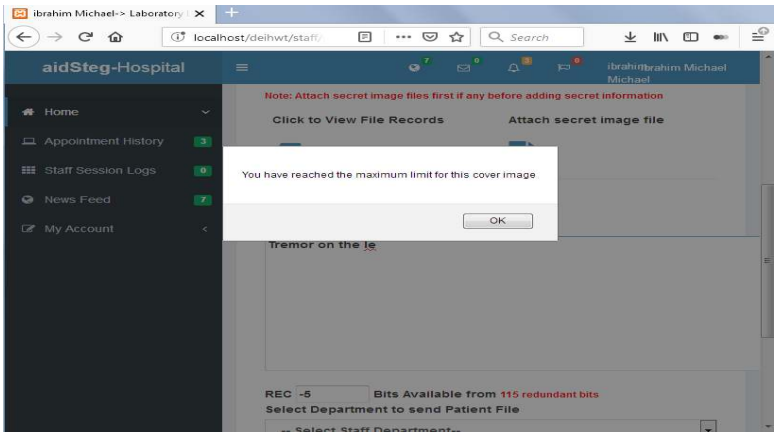
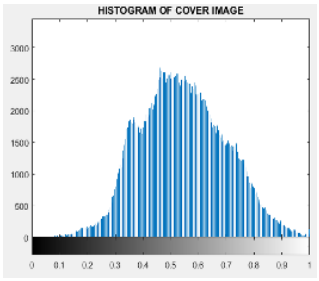


Figure 5: Real-Time Visualization of Redundant Bit Evaluator

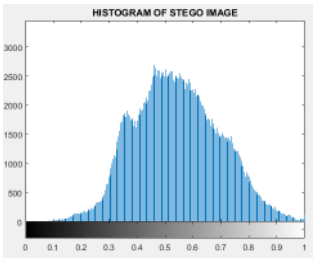
From Figure 5, it is seen that the available bits after concealing the patient passport in the Lena image are 115 bits. The developed REC deducts 8bits from the available redundant bit for any input or space inserted in the text field in real-time. The deduction will continue as long as a negative value is not obtained. A negative value will trigger the controller JavaScript to stop the embedding process as shown in Figure 5. Once the controller triggers, the input field becomes inactive for user access. More so, once any input is deleted or removed from the text field, 8bits are added to the remaining bits in real-time. After concealing both image and text as secret information in the Lena and pepper images, the cover-image and the generated equivalents stego-image qualities were evaluated using the developed AID MATLAB simulator shown in Figure 4. The histogram analysis of both cover and their respective stego-images is presented in Figure 6.

Corresponding author: Idakwo, M.A. ✉ *mondabutuj@gmail.com* ✉ *Department of Computer Engineering, Ahmadu Bello University, Zaria.*

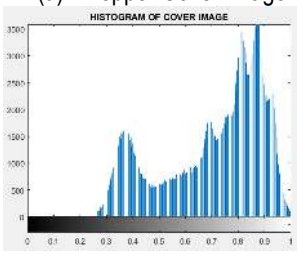
JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(2), JUNE, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com



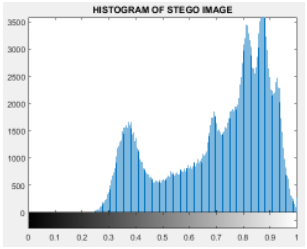
(a) Pepper Cover-image



(b) Pepper Stego-image



(c) Lena Cover-image



(d) Lena Stego-image

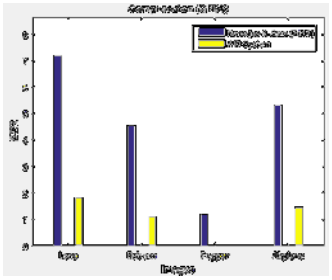
Figure 6: Histograms of Controlled Stego-Image using Redundant Bits Evaluator

From Figure 6, it is seen that the cover-images histogram bins of Figure 6(a) and Figure 6(c) histogram bins have no noticeable visual difference from their respective stego-images histogram bins in Figure 6(b) and Figure 6(d). This indicates that the developed real-time user-friendly redundant bits evaluator was able to control the image embedding rate to maintain a higher perceptibility rate. Equally the REC helps in the avoidance of truncating sensitive information. The developed redundant bits evaluator counter provides real-time visualization of the total available bits in a stego-image during the process of concealing the secret information. This is essential to avoid the truncation of any information.

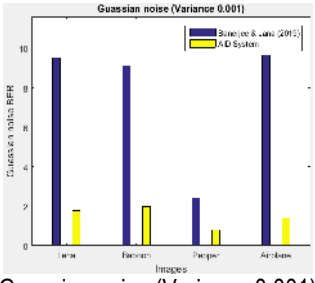
Robustness Analysis

It is essential to subject any new steganography technique to various attacks to evaluate the effect of such attacks on the embedded secret information. To effectively evaluate the developed steganography-based patient management information system against various attacks, the developed AID MATLAB simulator was used to perform a robustness analysis. The cover-images used for the evaluations are Lena, Baboon, Airplane, and Pepper. They were all used to conceal a secret logo with dimensions 75 by 75 and the equivalent generated images were all subjected to single and hybrid attacks (compression, rotation, Gaussian noise, cropping logo, salt and pepper attacks). The bits error rate in equation (1) was used to evaluate the degree of the respective attacks on the stego-images. The obtained results were compared with the results obtained from the techniques presented by Banerjee and Jana [27]. The comparisons are shown in Figure 7.

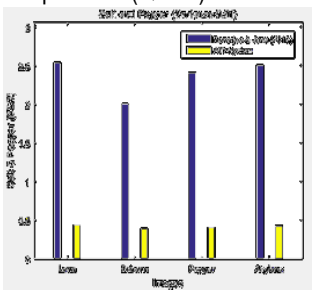
Corresponding author: Idakwo, M.A. ✉ *mondabutuj@gmail.com* ✉ *Department of Computer Engineering, Ahmadu Bello University, Zaria.*



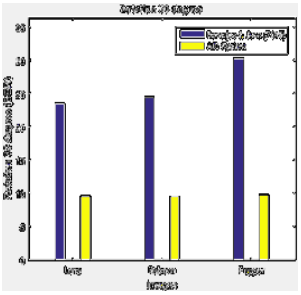
(a) Compression (QF 90)



(b) Gaussian noise (Variance 0.001)



(c) Salt and Pepper



(d) Rotation

Figure 7: System Robustness Analysis Test

The robustness analysis of the developed AID system and techniques implemented by Banerjee and Jana [27] presented in Figure 7 shows varying responses by the systems to the subjected attacks. In the AID System, the subjected attacks do not affect the embedded secret data as the embedded secret logo was retrieved but have a slight effect on the approximation coefficient of the stego-image. The reason for the non-effect on the secret data is because the developed AID algorithm conceals information majorly in the vertical, diagonal, and horizontal coefficients of the stego-image. The approximation coefficient is only used when the redundant bits in the vertical, horizontal, and diagonal coefficients are exhausted. The approximation coefficient usage is then subjected to a critical evaluation of all embeddable regions which will not distort the image. Therefore, the approximation coefficient is hardly used as it contains the cover-image digital image information. This accounts for the lower bits error value. The average responses of the systems to various attacks are as presented in Table 2.

Table 2: Comparison of Average Bits Error Rates (BER) Responses to Various Attacks

Single and Hybrid Attacks	Banerjee and Jana [27]	Aid System	Improvement (%)
Compression (QF=90)	4.59	1.62	64.71
Gaussian noise (V=0.0001	9.44	1.73	81.67
Salt and Pepper	2.36	1.0	57.63
Rotation	18.03	9.61	46.70
Cropping (25%) and Rotation (15%)	30.42	10.7	64.83
Salt and Pepper (v=0.01) + Guassian (v=0.001)	5.94	1.01	83.50

The BER as stated in equation (1) evaluates the ratio between the incorrectly extracted stego-image bits after and before an attack. A higher BER of an attack means a higher effect of such attack on the stego-image, this entails a lower system resistance to such attack. From the

Corresponding author: Idakwo, M.A. ✉ *mondabutuj@gmail.com* ✉ *Department of Computer Engineering, Ahmadu Bello University, Zaria.*

average bits error rates analysis shown in Table 2, it is seen that the developed system has a lower BER rate when compare to works of Banerjee and Jana [27], thus it is more robust against image steganalysis attacks compared to the state-of-the-art.

Secure Self Destructive Scheme

To evaluate the developed secure stego-image self-destructive scheme, a patient passport of dimension 450 by 450 was used to conceal a clinical test result. A wrong stego-key was used for the decoding process to see the effectiveness of the developed secure stego-key self-destructive scheme as shown in Figure 8.

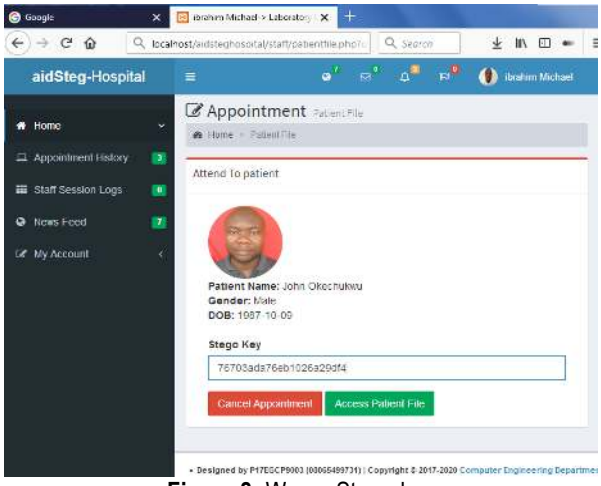


Figure 8: Wrong Stego-key

Once the access patient file button is clicked, the stego-image is immediately transformed into the frequency domain from the time domain and a stego-key match is performed. Since the input stego-key is not the same as the stego-key in the stego-image, the developed secure stego-image self-destructive scheme is triggered. This scheme will securely remove the concealed information. To validate this process, the stego-image after the wrong entry trial and the cover-image were evaluated using the IQMS panel on the developed AID MATLAB simulator. The cover-image was fed into the simulator using the select cover image on the simulator graphical interface. Equally, the stego-image was fed into the select stego image. The results obtained are presented in Figure 9.

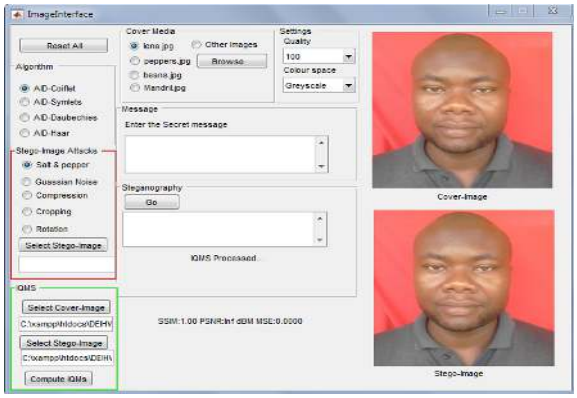


Figure 9: Image Qualitative Metrics for Wrong Stego-Key

Corresponding author: Idakwo, M.A. ✉ *mondabutuj@gmail.com* ✉ *Department of Computer Engineering, Ahmadu Bello University, Zaria.*

In Figure 9, it is seen that the structural similarity index metrics, PSNR, and MSE generated 1.00, inf, and 0.0000 respectively. The MATLAB psnr function only returns an inf value when two images are identical. The inf refers to infinity and it is due to a one-over 0 division. This can equally be verified from the PSNR equation presented in equation (4), as the log of 0 is infinity since the mean square error is 0. This indicates that the stego-image and the cover-image are identical. Recall that the cover-image has no information, which implies that the stego-image equally has no information. Thus the stego-image has been returned to its initial cover-image state. This will hinder access to the embedded sensitive confidential information.

Stego-key Strength Analysis

The developed true random number generator produces random hexadecimal numbers using its dynamic environment is dynamic that cannot be easily reproduced or manipulated. For instance, using the generated key in Figure 8 as an example; where k is 23 and the key is 76703ada76eb1026a29df4. A steganalyst will require 10^{23} x 23! Brute force attack once the environment which created the key is reproduced (i.e. mouse wait time, system date, and time in milliseconds) to generate the exact key. This implies that the stego-key total length is 184 bits (i.e. 8 x 23). Using this value, the duration for using brute force attack to break the system can be evaluated as follows:

$$Stego\_keys\_Lenght = 2^n \quad (8)$$

Where: n is the stego-key total length bits

$$Stego\_Key\_Lenght = 2^{184}$$

$$Stego\_Key\_Lenght = 2.452 \times 10^{55} keys$$

If a steganalyst is using a powerful computer like AMD Ryzen 7 processor which has the capacity of executing 304,510 MIPS per second, it takes time (T) to break the key once the environment which produced the key is reproduced.

$$T = \frac{2^{184}}{304510 \times 10^6 \times 60 \times 60 \times 24 \times 365} = 2.5533 \times 10^{36} (years)$$

The time taking to break into the system theoretically was compared with the keyspace analysis of Ogras [31] chaotic generator.

Table 3: key Space Analysis Comparison

Algorithm	Key Space	Breaking Time (Years)
Chaotic Generator	2^{100}	1.32×10^{11}
Developed System	2^{184}	2.5533×10^{36}

From Table 3, it is seen that the developed true random number generator has the highest duration of time (years) to break into the system. Therefore the developed system offers more security against brute force attacks

CONCLUSION

This paper has presented a steganography-based patient management information system. The developed system uses a novel real-time redundant bits evaluator counter to control information truncation, mouse wait time and system date time to generate stego-keys, and a non-separable integer-to-integer wavelet to decompose the patient information. The implementation of the system shows that it can be adopted to covertly convey patient diagnosis, prescription, and treatment thus solving the problem of patient information confidentiality and privacy.

REFERENCE

[1] Idakwo, M. A., Mu'azu, M. B., Adedokun, E. A., & Sadiq, B. O. (2022). Development of a Non-Separable Integer-to-Integer Wavelet Transform-Based Digital Image Steganography System. *Applications of Modelling and Simulation*, *6*, 20-27.

[2] Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Mohammed, K. I., Albahri, O. S., Albahri, A. S., & Alsalem, M. A. (2021). PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence

Corresponding author: Idakwo, M.A. ✉ mondabutuj@gmail.com ✉ Department of Computer Engineering, Ahmadu Bello University, Zaria.

architecture. *Multimedia Tools and Applications*, 1-25.

[3] Andreas, A., Mastorakis, G., Batalla, J. M., Sahalos, J. N., Pallis, E., & Markakis, E. (2021, October). Robust Encryption to Enhance IoT Confidentiality for Healthcare Ecosystems. In *2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1-6). IEEE.

[4] Moorthy, V. S., Roth, C., Olliaro, P., Dye, C., & Kieny, M. P. (2016). Best practices for sharing information through data platforms: establishing the principles. *Bulletin of the World Health Organization, 94*(4), 234.

[5] Payne-James, J. (2018). Confidentiality & consent in police custody: General principles. *Journal of forensic and legal medicine, 57*, 66-72.

[6] Chiwire, P., Evers, S. M., Mahomed, H., & Hiligsmann, M. (2022). Identification and Prioritization of Attributes for a Discrete Choice Experiment Using the Nominal Group Technique: Patients' Choice of Public Health Facilities in Cape Town, South Africa. *Value in Health Regional Issues*, *27*, 90-98.

[7] Lo, C. K., Chen, H. C., Lee, P. Y., Ku, M. C., Ogiela, L., & Chuang, C. H. (2019). Smart dynamic resource allocation model for patient-driven mobile medical information system using C4. 5 algorithm. *Journal of Electronic Science and Technology*, *17*(3), 231-241.

[8] Mbunge, E., Muchemwa, B., & Batani, J. (2022). Are we there yet? Unbundling the potential adoption and integration of telemedicine to improve virtual healthcare services in African health systems. *Sensors International*, *3*, 100152.

[9] Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., ... & Alhayani, B. (2022). Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience*, 1-14.

[10] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

[11] Govind, P. S., & Judy, M. V. (2021). A secure framework for remote diagnosis in health care: A high capacity reversible data hiding technique for medical images. *Computers & Electrical Engineering*, *89*, 106933.

[12] Dixit, P., Gupta, A. K., Trivedi, M. C., & Yadav, V. K. (2018). Traditional and Hybrid Encryption Techniques: A Survey *Networking Communication and Data Knowledge Engineering* (pp. 239-248): Springer.

[13] Manoj, R., Alsadoon, A., Prasad, P. C., Costadopoulos, N., & Ali, S. (2017). *Hybrid secure and scalable electronic health record sharing in hybrid cloud.* Paper presented at the 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud).

[14] Karakus, S., & Avci, E. (2020). A new image steganography method with optimum pixel similarity for data hiding in medical images. *Medical Hypotheses*, *139*, 109691.

[15] Zaheer, Z., Khan, A., Umar, M. S., & Khan, M. H. (2019). One-Tip Secure: Next-Gen of Text-Based Password *Information and Communication Technology for Competitive Strategies* (pp. 235-243): Springer.

[16] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access, 6*, 20596-20608.

[17] Santoso, B. (2019). *Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm.* Paper presented at the Journal of Physics: Conference Series.

[18] Ahmad, M. A., Elloumi, M., Samak, A. H., Al-Sharafi, A. M., Alqazzaz, A., Kaid, M. A., & Iliopoulos, C. (2022). Hiding patients' medical reports using an enhanced

Corresponding author: Idakwo, M.A. ✉ *mondabutuj@gmail.com* ✉ *Department of Computer Engineering, Ahmadu Bello University, Zaria.*

wavelet steganography algorithm in DICOM images. *Alexandria Engineering Journal*, *61*(12), 10577-10592.

[19] Chen, J., Lu, W., Yeung, Y., Xue, Y., Liu, X., Lin, C., & Zhang, Y. (2018). Binary image steganalysis based on distortion level co-occurrence matrix. *Comput. Mater. Contin, 55*(2), 201-211.

[20] Singh, S., & Gehlot, A. (2022). A data hiding technique for digital videos using entropy-based blocks selection. *Microsystem Technologies*, 1-10.

[21] Kumar, A. (2022). A cloud-based buyer-seller watermarking protocol (CB-BSWP) using semi-trusted third party for copy deterrence and privacy preserving. *Multimedia Tools and Applications*, 1-32.

[22] Atawneh, S., Almomani, A., Al Bazar, H., Sumari, P., & Gupta, B. (2017). Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. *Multimedia Tools and Applications, 76*(18), 18451-18472.

[23] Kurien, A. T. J., Mathew, S. A., & Mana, S. C. (2022, April). Development of PHP and MySQL based Digital Asset Management System for Secure Organizations. In *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 1859-1863). IEEE.

[24] Sisyukov, A. N., Dobrynin, V., & Yulmetova, O. S. (2021, January). Web Based GPU Acceleration in Embodied Agent Training Workflow. In *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)* (pp. 686-689). IEEE.

[25]Laperdrix, P., Starov, O., Chen, Q., Kapravelos, A., & Nikiforakis, N. (2021). Fingerprinting in style: Detecting browser extensions via injected style sheets. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 2507-2524).

[26] Banik, A., Shrivastava, A., Potdar, R. M., Jain, S. K., Nagpure, S. G., & Soni, M. (2022). Design, modelling, and analysis of novel solar PV system using MATLAB. *Materials today: proceedings*, *51*, 756-763.

[27] Banerjee, A., & Jana, B. (2019). A robust reversible data hiding scheme for color image using reed-solomon code. *Multimedia Tools and Applications, 78*(17), 24903-24922.

[28]Preishuber, M., Hütter, T., Katzenbeisser, S., & Uhl, A. (2018). Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Transactions on Information Forensics and Security, 13*(9), 2137-2150.

[29]Ghosal, S. K., Chatterjee, A., & Sarkar, R. (2020). Image steganography based on Kirsch edge detection. *Multimedia Systems*, 1-15

[30] Idakwo, M. A., Muazu, M. B., Adedokun, E. A., & Sadiq, B. O. (2020). An extensive survey of digital image steganography: state of the art. *ATBU Journal of Science, Technology and Education*, *8*(2), 40-54.

[31] Ogras, H. (2019). An Efficient Steganography Technique for Images using Chaotic Bitstream. *International Journal of Computer Network and Information Security, 11*(2), 21.

Corresponding author: Idakwo, M.A. ✉ mondabutuj@gmail.com ✉ Department of Computer Engineering, Ahmadu Bello University, Zaria.