ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 12(6), DOI: 10.17485/ijst/2019/v12i6/141437, February 2019*

An Improved Data Hiding Technique using Context Aware System

Majed Aborokbah*

Faculty of Computers and Information Technology, University of Tabuk, Tabuk City, Saudi Arabia; m.aborokbah@ut.edu.sa

Abstract

Objectives: The study presents a novel DH (Data Hiding) technique which is the combination of DH and context aware system (CAS) for developing/improving the conventional DH scheme. It ensures that the decoder/receiver authenticity before proceeding into the decode process. **Methods/Statistical Analysis:** This validation operation is performing in three different layers using the CAS properties. The decode action is performed based on the validation result by the proposed system at receiver side. In detail, if the decoder validation is success then he/she may permit to decode the encoded data by Modified Steganography for Image Decode (MSID) process else the system will give another chance to make their validation. If the validation is failed maximum of three times then the system will be deleted the encoded without the knowledge of the receiver. **Findings:** This feature has been added with the conventional DH system. The proposed system is divided into two different stages of DH and validation using CAS. The secret image is hiding inside of the known image using Modified Steganography for Image encode (MSIE) process and the validation parameters of the user name, location where the decode should be performed and time schedule are appended and it sent to the receiver in the sender side. He/she must perform the validation process and the CAS will take a decision based on the validation result once the receiver/decoder received the data. As the outcome of this system, the intruder can't be access the encoded data 99%, the strengthen ratio is improved up to 95% than the existing scheme, the secret data is reconstructed without any loss, it can ensure the reliability, availability and confidentiality of the secret data up to 98%. **Application/Improvements:** It has implemented for the clandestine image/data transmission between sender and receiver using CAS.

Keywords: Context Aware System, Data Hiding, Data Hiding Technique, Receiver, Secret Data, Sender

1. Introduction

Essentially, the DH is a technique where the clandestine image is hiding inside of a known/cover image for the secure transmission. As the outcome, the encoded image is look like the given cover image. The intruders may fails to hack data while transmitting due to this attitude. The medical image is considered as a secret image and it has sent to the authenticated user/receiver for the decode process. They had incorporated the new compression scheme which is suitable for the DH. As the outcome, they were claiming that their method is providing fast and secure transmission[4-6].

The paper had introduced the SDIHID scheme (Spatial-Domain Image Hiding using Image Differencing) in 2000. The deliberate technique is to implant a HI (Hidden Image) into a CI (Cover Image). The approach became supported by the parallel among the grey values in sequence of picture pixels variant insensitiveness from sleek to contrastive due to the truth of human visual order. An encoded image turned into generating by means of change the pixel values of a various results attained from the HI with those of a differencing outcome received from the secret image. The method preserves the HI with no loss and it produces the encoded with low degradation[7]. A Grey scale IH scheme based on VQ (Vector Quantization) had proposed in 2003. It is to decrease the amount of

*Author for correspondence

secret images to be fixed and the VQ topic was used to encode secret images. In addition, the compressed message was encrypted by way of the DES cryptosystem to affirm security. Lastly, the encrypted data was hidden into the secret image by grasping the LSB (least significant bit) substitution method[8]. The Histogram-based reversible DH for VQ compressed images has introduced in 2009. The article was saying that, the reversible message hiding activity is needed and suitable in numerous applications like diagnosing, law enforcement, military and creation work etc[9]. The ROI based error concealment of a compressed object based image using QIM DH and wavelet transform was developed in 2010. The strategy is that, the transmission of digital data through radio cellular channel was evidencing a weakening result that consequences in severe decadence in first-class. Error hiding changed into a post refinement method to enhance this excellent degradation[10]. The RDH in encrypted image (RDEI) was introduced in 2011. This work presents a completely unique RDH theme for the encrypted image. Later encrypting the complete information of uncompressed image by stream encoding technique, the extra data may be embedded into the image by editing a small part of encrypted data[11] and the reversible and high-capacity DH in medical images was also proposed in 2011[12].

A survey on the security and privacy issues related with the CAS's was presented in 2012. It was describing various security requirements for the CAS, such as the confidentiality and privacy requirements are essentially related to protect the use of some highly sensitive information or data and various frameworks for evolving well-organized and effective security on user's information using CAS had proposed[13]. Architecture for CA (Context Aware) web services based on privacy preferences is developed by the authors and the aims were to contribute privacy management layer to the CAWSA (CA Web Service Architecture) and the purpose of privacy management layer is to hearten the concept of privacy awareness in it[14]. The paper projected the concept of any one can right to safeguard their information or services to the user environment and service conditions. The reflection of user privacy predilections in provision of CA web services was addressed in this paper and the consumer secrecy language was presented with an adaptation mechanism for SOAP messages[15]. Another paper had presented a CA secrecy protection system for LBS (Location Based Services). The design of secrecy maintaining techniques was principled in terms of time and space complexities. In addition, the CA secrecy protection system with Google maps, LBS[16] had introduced. A framework for CA privacy of sensor data on mobile system and privacy was needed when a user shares personal sensor data with applications on a smartphone in it. It focuses on the more general problems of choosing what data to share, in such a way that certain kinds of inferences[17]. The author described the context protecting privacy preservation in ubiquitous computing, because CA was an important issue in ubiquitous computing domain[18]. They had projected a scheme which provides two layer privacy protection of user's or application's context data. The paper presented a method of predicting the secrecy concern based on an index model of privacy and also an approach method of triggering the secrecy preserving service[19]. The CA retrieval points of interest, it's a popular LBS. The access to points of interest services is prone to potentially serious privacy issues[20]. The paper had described reviews of research and analyses were about the effect of threat on the secrecy of CAS users. They proposed a framework to tackle the privacy preservation issue lengthily, from user viewpoint as well as service provider view[21].

2. Hybrid Data Encode and Context Aware System

The paper has proposed a DH technique for the medical applications[2]. It was one of the efficient techniques where the secret image can be transmitted in an effective manner. Though, the paper proposes a new DH technique which is the combination of the CAS features. It's also called Hybrid DH and CAS. The CAS is a component of a ubiquitous computing or pervasive computing environment. In addition, it has three important aspects of context are as follows[1]:

- Where you are,
- Who you are with and
- What resources are nearby?

The main aim of this work is that, the decode process performs according to the following validations,

- The person-who is doing the decode process
- Location-where the action is performing and
- Time of the process

The reconstruction of the secret data is not an easy task if any one of these three fails. In detail, the proposed

system can be classified into two parts, one is performing at the sender side and another one is performing at the receiver side. The secret image is hidden into the cover image and the validation information's (CAS) are appended with the encoded image as given in the Equation 1. It is sent to the receiver for the reconstruction process by the encoder/sender. The system validates based on the three constrains one by one for ensuring the user authenticity. If any one of these three constrains fails, it will give another two chances for the same validation processes. If its successfully validated then the encoded data will be decoded else the process will be terminated and the received data will be deleted without the knowledge of the receiver at receiver side.

2.1 Sender Side Process

The sender side process is divided into two processes of Image encode process and preprocess of CAS as illustrated in the Figure-1. There are two input images of secret and cover images are considered for the encode process. The secret image is embedded into the cover image using MSIE process[2].

$$Encode\left[\sum_{i=0,j=0}^{m,n} C \oplus \sum_{i=0,j=0}^{m,n} S\right] || \, ICAS = \sum_{i=0,j=0}^{m.n} E \quad (1)$$

This process is performing in various stages of Segregation/splitting subbands, Binary Conversion (BC) Process, Substitution Process, and Decimal Conversion (DC) Process as mentioned in the Figures 1 and 2.

- *Split Subbands*

The secret and cover images are considered an input for this process. Each image is split into 2x2 levels of the

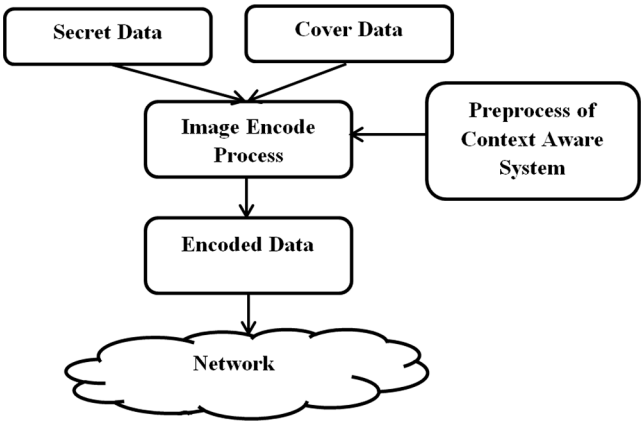

Figure 1. Sender side Process.

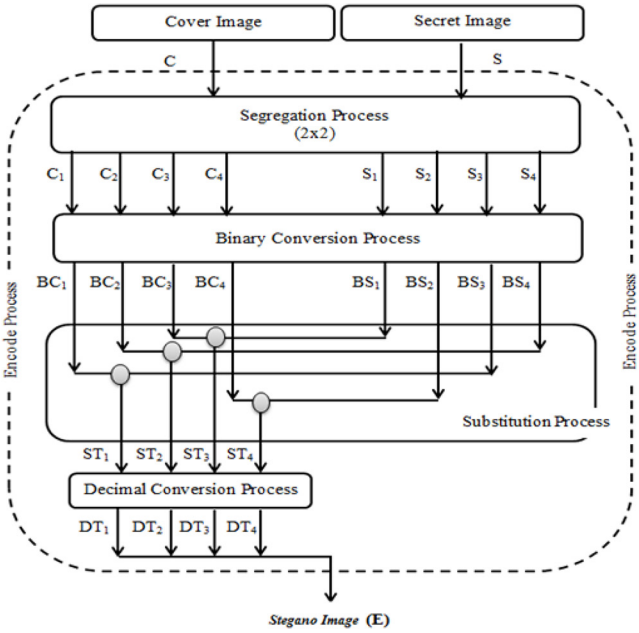

Figure 2. MSIE Technique.

subabnds. As the result, the secret and cover images are split into 4 different parts.

- *BC Process*

The split subbands of the secret and cover pixels are converted into corresponding 8bits binary values in this stage.

- *Substitution Process*

The converted secret bits are substituted instead of the cover LSB. It means every cover LSB are replaced by the secret bits which is based on the Algorithms I and II[2,3] in this stage and it is an important stage of the DH.

- *DC Process*

Every 8bits are converting into the equivalent decimal value after the bit substitution process in DC process. The BC, substitution and DC processes are performing separately for every pair of the sub bands. As the result of the substitution process is binary sub bands and these sub bands binary values are converted into the equal decimal value and it has been illustrated in the Figure 2. Finally, the four sub bands are joint as an image and it is also called an encoded image as shown in the Figure 3.

$$P \oplus L \oplus T = ICAS \quad (2)$$

The encoded image is appended with the ICAS validation parameters of Person details P, Location L and Time

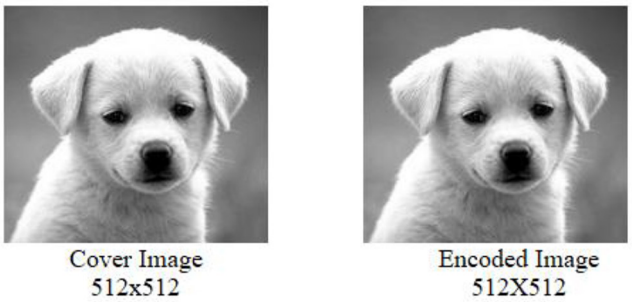

Figure 3. The Cover and Encoded Images.

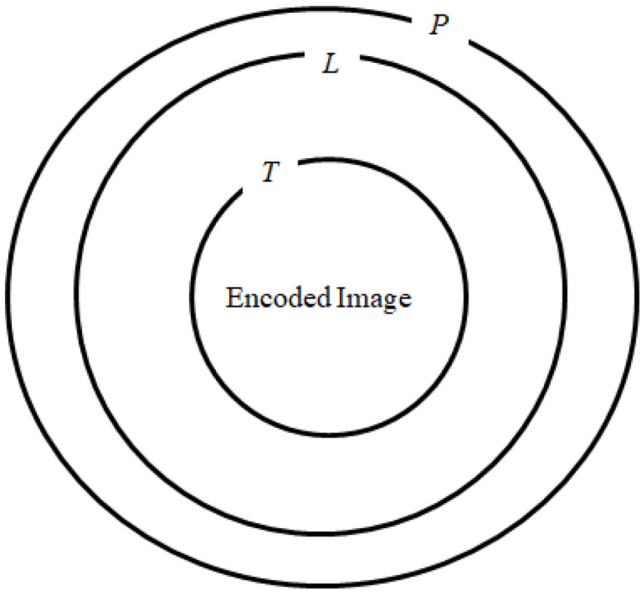

Figure 4. The validation layers.

T in the second stage of the sender side process as given in the Equations 2 and Figure 4. It facilitates the user decode validation during the decode process at the receiver side.

Personal details: The authenticated user who is going to decode the secret data is described by *P*.

$$P = Uname \tag{3}$$

It is the first validation of the reconstruction process as mentioned in Equation 3.

Location: The location where supposed to be decoded by the authenticated user is described by *L*.

$$L = Location(Uname) \tag{4}$$

The user location is acquiring with the help of GPS (Global Positioning System) during the validation and it is matching with the predefined location in the second stage as given in Equation 4.

Time: The specific decode time is defined by the *T* and it's also known as third validation, as given in Equation 5.

$$T = Time(Decode) \tag{5}$$

The encoded data $\sum_{i=0,j=0}^{m.n} E$ is sent to the receiver side once all the validation information's are enclosed in it.

2.2 Receiver Side Process

Traditionally, the received encoded data is decoded for reconstructing the secret and cover data's. Nevertheless, Narmatha et. al. have proposed an efficient decode techniques which is suitable for MSIE. This technique is perfectly reproducing the secret and cover images[3]. It has been incorporated in receiver side process for the data reconstruction. The receiver side process has been classified into two stages. The receiver who is going to reconstruct the secret data is validating before the reconstruction process for improving the user authenticity based on the following validation process in first stage. The secret data is reconstructing by MSID if the user validation is successfully else the encoded data will be deleted automatically without the knowledge of the receiver. Finally, the reconstructed secret data is validating for ensuring the integrity as denoted in the Figure 5.

CAS Validation Process

There are three layers validations have been incorporated in this system which is based on the CAS as follows. The receiver name is validating with the given system name if the name is successfully validated then the user

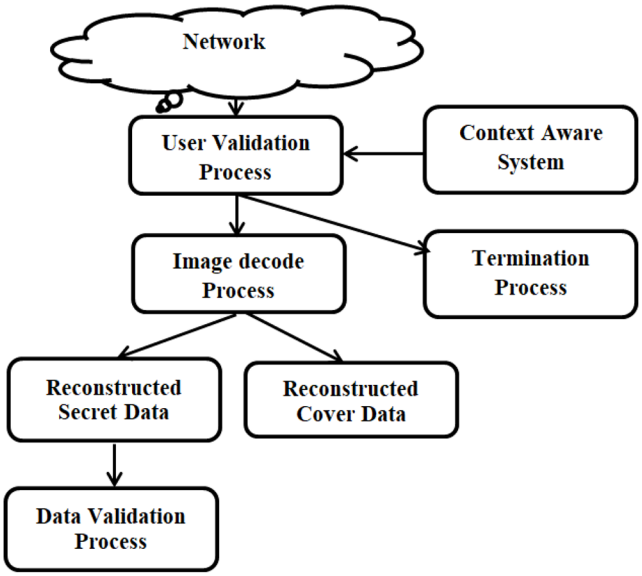

Figure 5. Receiver Side Process.

correct location which is acquired by the GPS and the given location in the system are compared if the matching is success then the current time of the system and predefined time are validating is both times same then the system permits the receiver to reconstruct or decode the encoded data else the received data will be deleted automatically without the knowledge of the receiver at the receiver side as illustrated in Figure 6. The user who is going to decode the encoded data is validating before proceeding reconstruction process and the user authenticity also been improved due to this operations.

MSID Process

The MISD process can be divided into the segregation/fragmentation, BC, Inverse Substitution and DC Processes[3] as mentioned in the Figure 7.

- ***Fragmentation Process***

The encoded data is segregated into four equal sub bands once the validation process is over. As the outcome, there are four equal sub bands created.

- ***BC Process***

The segregated sub bands every pixel is converted into corresponding 8bits binary values in this process. The outputs of this process are considered as the inputs for the inverse substitution process.

- ***Inverse Substitution Process***

The LSB bits of every pixel are replaced for creating the secret data sub bands in this process as per the algorithms[3]. As the result, there are four equal binary sub bands of secret and cover images generated. It is also known as the reverse process of the substitution.

- ***DC Process***

```
If p(uname) = Receiver uname then
{
   if (L(Uname))=current position of the user then
         {
            If  (T(decode))=  Current  Decode  Time
               then
                        {  Execute decode process}
         }
}
Else    {       Delete Encoded data
               Don't acknowledge to Receiver
         }
```

Figure 6. The Pseudocode of the Validation.

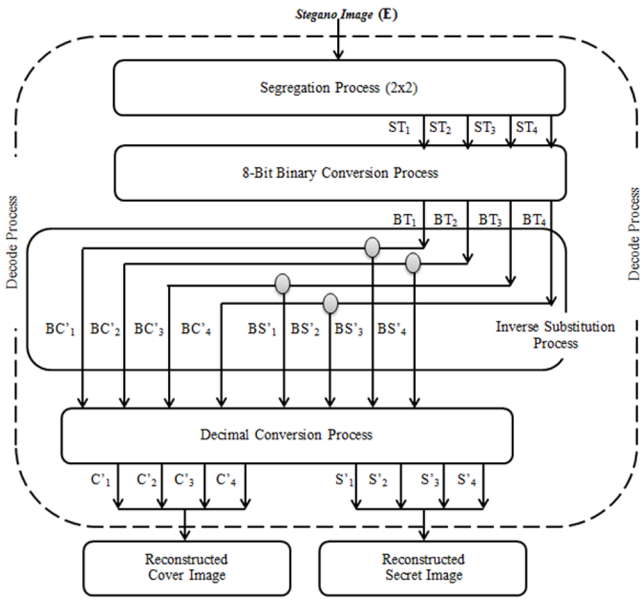

Figure 7. MSID Technique.

Every sub bands8bits of secret and cover are converted into the corresponding decimal value. In addition, the secret sub bands are merged as an image and the same operation has done for generating the cover image as well.

3. Experimental and Result Discussion

There 1000 sample data's are considered for evaluating the proposed system performance with traditional/conventional system. The gray scale secret and cover images are input in this experimentation and all are in. bmp (bitmap) format as given in the Figures 8 and 9. The time of encode and decode, accuracy rate, user authentication level, data integrity level and complexity level are considered for evaluating the proposed system performance with the traditional system. The standard steganography is called a traditional system.

The working principle of the proposed system is that, there are two images are playing an important role in DH and those images are secret and cover. The size of the secret and cover images ratio is 1:2. It means that the cover image size should be double of the secret image size for encode and decode processes as mentioned in the Figures 8 and 9.

The proposed system is consuming the minimum execution times than the conversional system while comparing based on encode and decode times. It has been illustrated in Figures 10 and 11. The Figure 12 and

Figure 8. Sample of Cover Images (512x512).

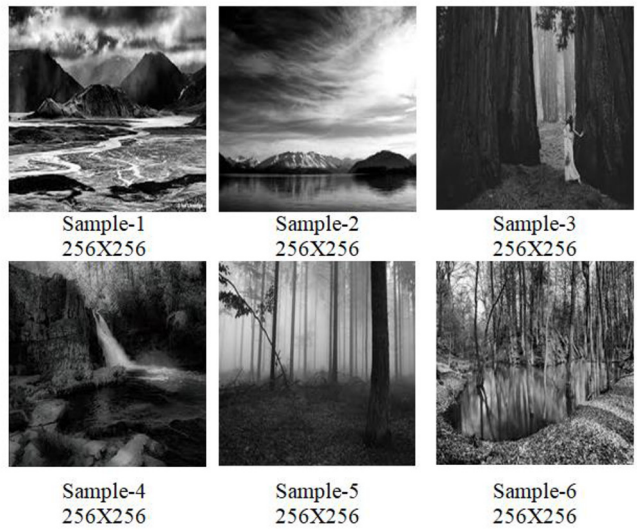

Figure 9. Sample of Secret Images (256x256).

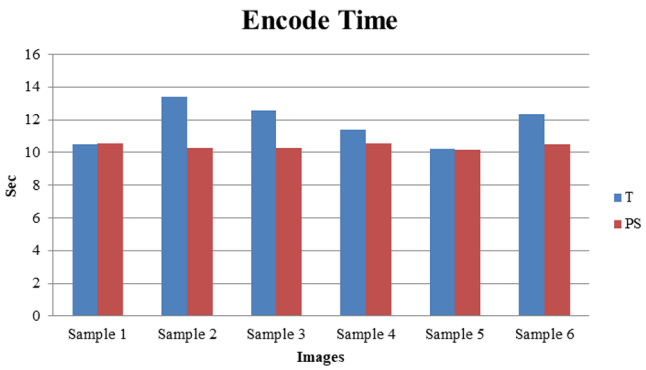

Figure 10. The Encode Times.

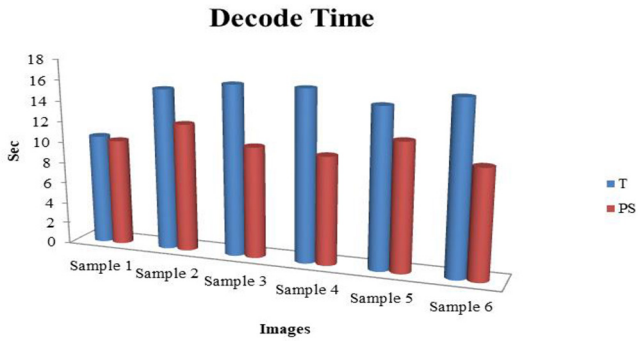

Figure 11. The Decode Times.

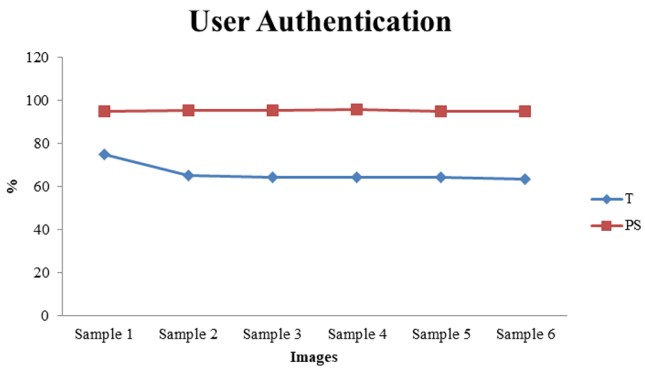

Figure 12. The User Authentication level Analysis.

Table-1 clearly shows that the proposed system is providing the high authenticity compared than the conventional system. The reason is that, the recevier/decoder authentication is not validating in convensional system. But, the proposed system is validating the user authenticity before decode the encoded data. This is one of the main advantage and strengthen of the proposed system. If the system complexity level is increased altimatly the strengthen will be increased.

So it is not an easy task to understand the encoded data by third parties/intruders. As the result, the secure transmission can be provided. The Figure 13 clearly indicating that, the proposed system complexity exstended than conventional. The reconsructed data integrity level has validated at the end for ensuring the exact replica of the secret image is reconstructed as mentioned in Figure 14. The proposed system has done a best role than the conventional scheme in it.

4. Conclusion

There is a chance that, the encrypted clandestine data may be accessed by the third parities/intruders for knowing

Table 1. Performance Analysis of Proposed System with Traditional System

Images		Encode Time (Sec)		Decode Time (Sec)		Complexity		User Authentication %		Data Integrity %	
C	S	T	PS	T	PS	T	PS	T	FPS	P	T
512x512	256X256										
S1	S1	10.5	10.56	10.5	10.2	7.1	9.25	75	95	89	92.68
S2	S2	13.4	10.25	15.45	12.25	7.5	9.15	65	95.45	87	92.56
S3	S3	12.54	10.27	16.24	10.58	6.5	9.2	64.5	95.28	87.25	92.68
S4	S4	11.41	10.54	16.25	10.25	6	9.35	64.25	95.68	86.99	92.25
S5	S5	10.24	10.14	15.11	12.12	7.34	9.52	64.38	95.01	87.5	92.11
S6	S6	12.35	10.47	16.25	10.35	7.2	9.87	63.25	95.07	87.36	94.25

T- Traditional System
C-Cover Image
PS-Proposed System
S-Secret image
Sec-Second

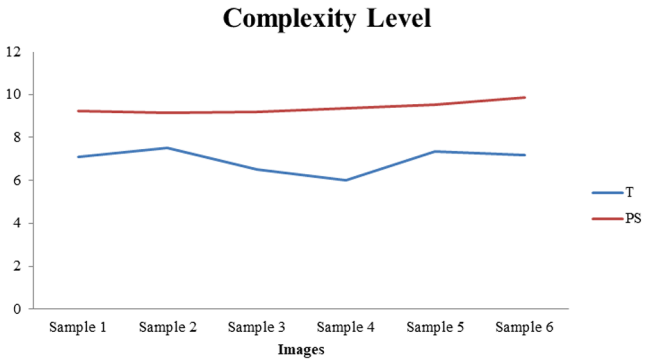

Figure 13. The system complexity level.

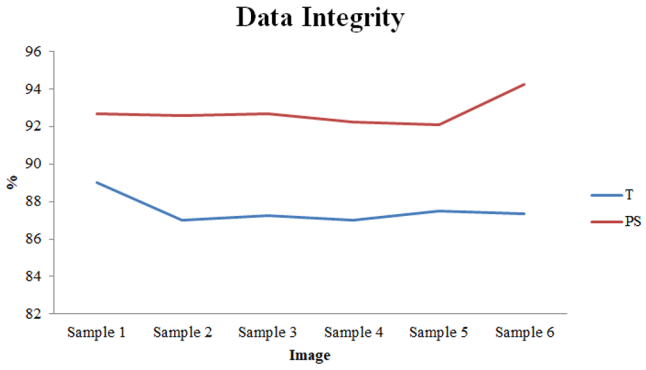

Figure 14. The Data Integrity.

the secret information when secret data are transmitting among the trusted users. The main problem of the system is that the data will be encoded in a perfect manner and it will be sent to the other side for the decode process. The unauthorized user will try one or more times to decode the data successfully if he received the encoded data. This study proposes an image hiding scheme with context aware system to solve this crucial issue. It validate the decoder before decode the encoded data. If it fails the secret data is deleted automatically without the prior notice to the unauthorized receiver. It is one of the main advantages. One of the efficient DH scheme is incorporated in this system along with context aware system. As the result, the clandestine data can be transmitted 96% securely, ensure that the authorized user only can reconstruct the data, the data integrity ratio is increased up to 97%, before the decode process the decoder is validating by the efficient validation process using context aware system and it provides perfect reconstruction process without any loss. In future, this system can be used for the defense applications with some modifications.

5. Acknowledgement

The author thanks the faculty of Computers and Information Technology, University of Tabuk, Tabuk City, Saudi Arabia for providing immense support and facilities for this work.

6. References

1. Thyagaraju GS, Umakant P Kulkarni. Design and Implementation of User Context aware Recommendation Engine for Mobile using Bayesian Network, Fuzzy Logic and Rule Base. International Journal of Computer Applications. 2012; 40(3):47-63.

2. Narmatha C, Manimegalai P and Manimurugan S. A Grayscale Image Hiding Encode Scheme for Secure Transmission. Current Signal Transduction Therapy. 2018; 13:1-6.
3. Narmatha C, Manimegalai P and Manimurugan S. A Decode Technique of MSI for Efficient Reconstruction Process. International Journal of Engineering & Technology. 2018; 7(3.6):110-4.
4. Manimurugan S and Narmatha C. Secure and Efficient Medical Image Transmission by New Tailored Visual Cryptography Scheme with LS Compressions. International Journal of Digital Crime and Forensics (IJDCF). 2015; 7(1):26-50. https://doi.org/10.4018/IJDCF.2015010102
5. Manimurugan S, Porkumaran K, Narmatha C. The New Block Pixel Sort Algorithm for TVC Encrypted Medical Image. Imaging Science Journal. 2014 Sep; 62(8):403-14.
6. Narmatha C, Manimegalai P and Manimurugan S. The Secure Lossless Compression Scheme for Grayscale Medical Images Using PBT and Modified Steganography. Journal of Advanced Research in Dynamical and Control Systems. Recent Trends in Engineering and Managerial Excellence. 2017 May; (3):96-103.
7. Wu DC and Tsai WH. Spatial-domain image hiding using image differencing. IEE Proceedings - Vision, Image and Signal Processing. 2000 February; 147(1). https://doi.org/10.1049/ip-vis:20000104
8. Yu Chen Hu. Grey-level image hiding scheme based on vector quantization. Electronics Letters. 2003 23rd January; 3(2):202-3.
9. Tsai P. Histogram-based reversible data hiding for vector quantisation-compressed images. IET Image Process. 2009; 3(2):100-14. https://doi.org/10.1049/iet-ipr.2007.0220
10. Amit Phadikar, Santi P Maity. ROI Based Error Concealment of Compressed Object Based Image using QIM Data Hiding and Wavelet Transform. IEEE Transactions on Consumer Electronics. 2010 May; 56(2). https://doi.org/10.1109/TCE.2010.5506028
11. Xinpeng Zhang. Reversible Data Hiding in Encrypted Image. IEEE Signal Processing Letters. 2011 April; 18(4):255-8. https://doi.org/10.1109/LSP.2011.2114651
12. Fallahpour M, Megias D, Ghanbari M. Reversible and high-capacity data hiding in medical images. IET Image Process. 2011; 5(2):190-7. https://doi.org/10.1049/iet-ipr.2009.0226
13. Almutairi S, Aldabbas H and Abu-Samaha A. Review on the security related issues in context aware system. De Montfort University, software technology research laboratory (STRL) Leicester, United Kingdom. Proceedings of the International Journal of Wireless & Mobile Networks (IJWMN). 2012 June; 4(3).
14. Gaud N, Deen A, Silakari S. Architecture for discovery of context-aware web services based on privacy preferences. Computer Science & Engineering, U.I.T, R.G.P.V. Bhopal, Madhya Pradesh, India. Proceedings of the Fourth International Conference on Computational Intelligence and Communication Networks. 2012. https://doi.org/10.1109/CICN.2012.52
15. Kapitsaki GM. Reflecting user privacy preferences in context-aware Web Services. Department of Computer Science University of Cyprus Nicosia, Cyprus. Proceedings of the IEEE 20th International Conference on Web Services. 2013. https://doi.org/10.1109/ICWS.2013.26
16. Aniket Pingley George, Wei Yu, Nan Zhang George, Xinwen Fu and Wei Zhao. A context-aware scheme for privacy-preserving location-based services. The International Journal of Computer and Telecommunications Networking Archive. 2012 July; 56(11):2551-68.
17. Chakraborty S and Raghavan KR, Johnson MP, Srivastava MB. A Framework for Context-Aware Privacy of Sensor Data on Mobile Systems. University of California, Los Angeles. ACM HotMobile'13, 2013 February 26-27. https://doi.org/10.1145/2444776.2444791
18. Ukil A. Context Protecting Privacy Preservation in Ubiquitous Computing. Innovation Labs, Tata Consultancy Services, Kolkata, India. Proceedings of the IEEE CISIM 2010, Krakow, Poland. https://doi.org/10.1109/CISIM.2010.5643649
19. Lee Y, Kwon O. An index-based privacy preserving service trigger in context-aware computing environments. School of International Management, Kyunghee University, Seochun, Ghiheung, Yongin, Kyunggi-do, South Korea. Expert Systems with Applications. 2010; 37:5192-200. https://doi.org/10.1016/j.eswa.2009.12.072
20. Riboni D, Pareschi L and Bettini C. Integrating Identity, Location, and Absence Privacy in Context-aware Retrieval of Points of Interest. University, degli Studi di Milano, D.I. Co., EveryWare Lab. 12th IEEE International Conference. 2011; 1. https://doi.org/10.1109/MDM.2011.17
21. Pandit AA and Kumar A. Conceptual Framework and a Critical Review for Privacy Preservation in Context Aware Systems. Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover IEEE. 2012; p. 435-42. https://doi.org/10.1109/CyberC.2012.79