Steganography of Messages Encrypted With QR Code

Ms. D Betteena Sheryl Fernando[1], Parthiban A[2], Rajesh R[3], Vinithra M[4]
[1]Assistant Professor, Dept of Computer Science and Engineering
Dept of Computer Science and Engineering
[1, 2, 3, 4] Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India

Abstract- *Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. In this paper, we present a QR code as a secret message to increase the embedding capacity and information security of the image steganography. we use quick response (QR)code. QR codes generated by our proposed system can carry its ordinary message in addition to the payload. Anyone can read the message, but the payload can only be obtained using a secret key. The message and the payload are unrelated; i.e. any message can be generated regardless of the payload and vise versa. We can take advantage of that by generating a message that gives misleading information to the adversary. we test the proposed system and show that the generated QR code is (valid) i.e indistinguishable from an ordinary QR code which makes it look innocent and less susceptible.*

Keywords- QR code, Steganography, Encryption, Decryption

I. INTRODUCTION

The necessary info like email passwords or bank details square measure transmitted on the net all the time. Those info should be protected to forestall it from falling within the wrong hands. Steganographic techniques is impelled by weaknesses in secret writing systems. Steganographic techniques are often wont to transmit the key info undetected , not like secret writing that makes the cipher text detectable and at risk of attacks. Steganography work as two lines of defense to guard the knowledge against associate opposer.

Cryptography is that the method of securing info throughout transmission. The sender is process it during a means that creates it indecipherable. The generated cipher text contains a uniform distribution It are often solely decrypted employing a secret key. generally securing info isn't enough, and activity its existence may be a should. For example, quantum computing, once absolutely developed will bused to crack and rewrite encrypted info. Moreover, some governments enforce laws that limit the employment of cryptological techniques or forestall it along. This created people and firms to seem for different alternatives. Multimedia like pictures square measure most popular containers to cover the payload as a result of they will face up to some distortion degree without poignant their quality. This created people and firms to seem for different alternatives. Businesses begin to know the potential of steganography; activity info regarding new merchandise within associate innocent-looking family photograph is a smaller amount suspicious than transferring associate encrypted file. it's most popular to write the payload before embedding it during a instrumentality to induce security from each worlds of steganography and cryptography . The encrypted payload, if detected, will seem as random noise since the encrypted message contains a uniform distribution. Moreover, if the payload is with success recovered then the payload remains indecipherable. a possible of steganography that has not nevertheless been absolutely used.

1. QRCODE

FIG 1. QR Code.

2. QR CODESTRUCTURE

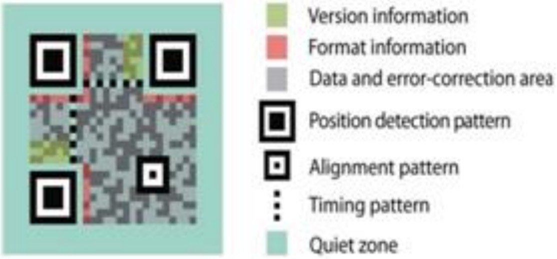


FIG 2. QR Code structure.

A quiet zone that may be a border of empty house needed for reading the QR code. The quiet zone is employed to ease the image detection. info info that determines the mask pattern and therefore the error correction level utilized in the QR code. A temporal arrangement pattern that acknowledges the central coordination of every cell with alternating black and white patterns. It corrects the central coordination of the cell once it's distorted or once there's miscalculation within the cell space.

II.RELATEDWORKS

Liao et.al. planned a medical joint photographic specialists cluster (JPEG) image steganographic system supported the dependencies of inter-block coefficients. Their system depends on keeping the deferences between the separate relative remodel (DCT) within the same place in neighboring DCT blocks as shut as potential. within the embedding method, the values are appointed dynamically in line with the alterations of inter-block neighbour‟s.

Sahu and young man conferred a steganographic system supported component worth differencing (PVD) and LSB. it's targeted on the error block downside (EBP) and FOBP. The image is divided into blocks with 2 adjacent pixels. The blocks ar split into 3 levels subject to the distinction of component values. The block level and therefore the component distinction verify the embedding capability of the block. Their system improves PSNR and embedding capability. additionally, the system is resistant to component distinction bar chart (PDH) analysis.

Rachmawantoet.al. enforced a security system that merges between cryptography by exploitation one-time parole (OTP), vernam coding and steganography by exploitation DCT during a digital image . Their system is tested exploitation PSNR and normalized cross correlation (NCC) to check the standard of the decrypted message. Their system is immune against JPEG compression and median filters.

Muhammad et.al. conferred a picture steganographic system that relies on stego key- directed adaptational least vital bit (SKA-LSB). In their system, a secret's encrypted employing a two-level coding algorithmic program (TLEA). After that, the message is encrypted employing a multi- level coding algorithmic program (MLEA), then the encrypted payload is hid within the host image exploitation associate adaptational LSB substitution. Their system achieves an inexpensive balance between quality and security.

Dey et. al. conferred a steganographic system that relies on a irregular intermediate QR host that's embedded with associate encrypted payload. First, the payload is encrypted then hid during a QR code. Then, the QR code is hidden within a picture. exploitation double coding and embedding techniques makes the system exhausting to interrupt. however on the opposite hand, it makes the system less time-efficient.

Rani at.al. planned a secure system within which they combined between steganography and QR codes. Their system consists of 2 elements. the primary one is making a QR code of the encrypted payload. The other is concealing the generated QR code within a coloured image. The concealing method doesn't generate an obvious image distortion and generates a really negligible bit error rate (BER).

Barrera et.al. enforced a system that uses QR codes in optical coding as containers. They opt for QR codes as containers in their system thanks to their tolerance to waste matter speckle noise. additionally, QR codes ar straightforward to scan exploitation cell phones‟ cameras. The results show that their system is additional vulnerable to noise compared to traditional optical encryption.

III. PROPOSEDMETHODOLOGY

After analyzing the wants of the task to be performed, ensuing step is to research the matter and perceive its context. the primary activity within the part is finding out the prevailing system and different is to know the wants and domain of the new system. each the activities square measure equally necessary, however the primary activity is a basis of giving the practical specifications so productive style of the planned system. Understanding the properties and needs of a replacement system is tough|harder|tougher} and needs creativeness and understanding of existing running system is additionally difficult, improper understanding of gift system will lead diversion from resolution.

1.HMAC-SHA256

A Hash Message Authentication Code (HMAC) perform could be a technique for substantiating the integrity of a message transmitted between 2 parties that agree on a shared secret key. primarily, HMAC combines the first message and a key to cipher a message digest perform. The sender of the message computes the HMAC of the message and also the key and transmits the HMAC with the first message. The recipient recalculates the HMAC exploitation the message and also the secret key, then compares the received HMAC with the calculated HMAC to ascertain if they match. If the 2 HMACs match, then the recipient is aware of that the first message has not been changed as a result of the message digest hasn't modified, which it's authentic as a result of the sender knew the shared key, that is likely to be secret. Any cryptographical hash perform, like SHA-2 or SHA-3, perhaps employed in the calculation of associate HMAC; the ensuing macintosh algorithmic program is termed HMAC-X, wherever X is that the hash perform used (e.g. HMAC-SHA256 or HMAC-SHA3-256). The cryptographical strength of the HMAC depends upon the cryptographical strength of the underlying hash perform, the dimensions of its hash output, and also the size and quality of the key. HMAC uses 2 passes of hash computation.

The secret secret's 1st accustomed derive 2 keys – inner and outer. the primary pass of the algorithmic program produces an enclosed hash derived from the message and also the inner key. The second pass produces the ultimate HMAC code derived from the inner hash result and also the outer key. so the algorithmic program provides higher immunity against length extension attack. associate unvarying hash perform breaks up a message into blocks of a set size and iterates over them with a compression perform.

- HMACs square measure generally abundant quicker to calculate and verify than digital signatures as a result of they use hash functions instead of public key arithmetic.
- They're so ideal for systems that need high performance, like routers or systems with terribly slow or tiny microprocessors, like embedded systems.
- HMACs square measure abundant smaller than digital signatures nevertheless provide comparable signature security as a result of most digital signature algorithms square measure accustomed sign cryptographical hash residues instead of the first message.
- HMACs can be used in some jurisdictions where the use of public key cryptography is legally prohibited or in doubt. To use and handle keys in a simple way.
- To have a well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions on the underlying hash function.
- To allow for easy replace ability of the underlying hash function in case that faster or more secure hash functions are found or required.

2. XTEA:

In steganography, XTEA (eXtended TEA) may be a block cipher designed to correct weaknesses in TEA. Like TEA, XTEA may be a 64bit block Feistel cipher with a 128-bit key and a steered 64 rounds. many variations from TEA square measure apparent, together with a somewhat additional complicated key-schedule and a transcription of the shifts, XORs, and additions. conferred at the side of XTEA was a variable-width block cipher termed Block TEA, that uses the XTEA spherical perform, however Block TEA applies it cyclically across a whole message for many iterations. as a result of it operates on the complete message, Block TEA has the property that it doesn't want a mode of operation. Associate in Nursing attack on the complete Block TEA was delineate in (Saarinen, 1998), that conjointly details a weakness in Block TEA's successor, XTEA.

3. MODELING ANDANALYSIS

In this half the system design and therefore the method that square measure concerned within the complete implementation of steganography of encrypted messages within valid QR codes exploitation encryption and decryption ways.

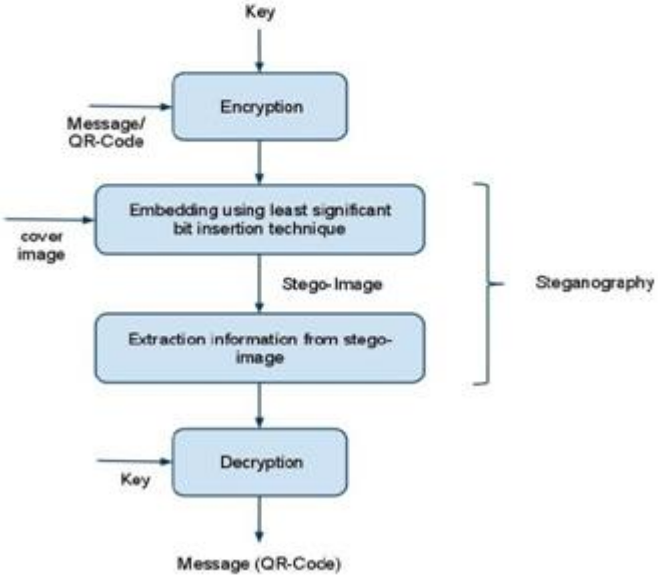

Key
Encryption
Message/
QR-Code
Embedding using least significant bit insertion technique
cover image
Stego-Image
Steganography
Extraction information from stego-image
Decryption
Key
Message (QR-Code)

FIG 3. System architecture of encryption and decryption. The system architecture of encryption and decryption is explained in detail in the following steps: 1) Creating a text file with secret data. 2) Embedding both text and qr code along with mac password. 3) Extract the embedded qr code along with mac password and key for decryption.

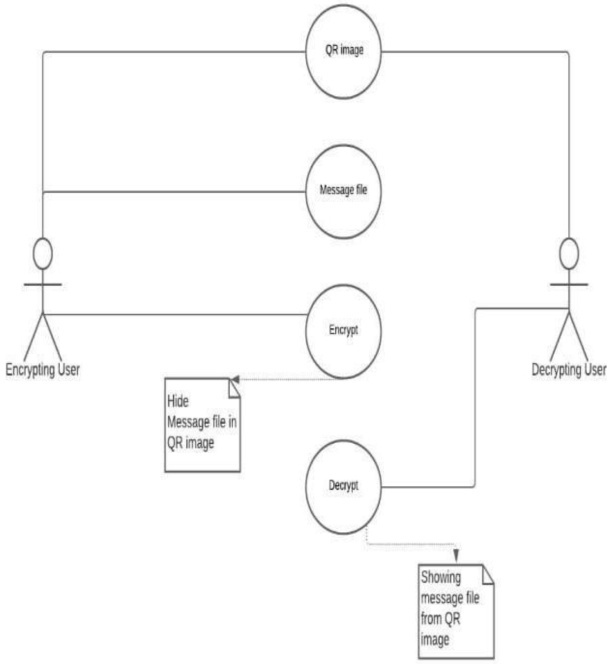


FIG 4. UMLDiagram.

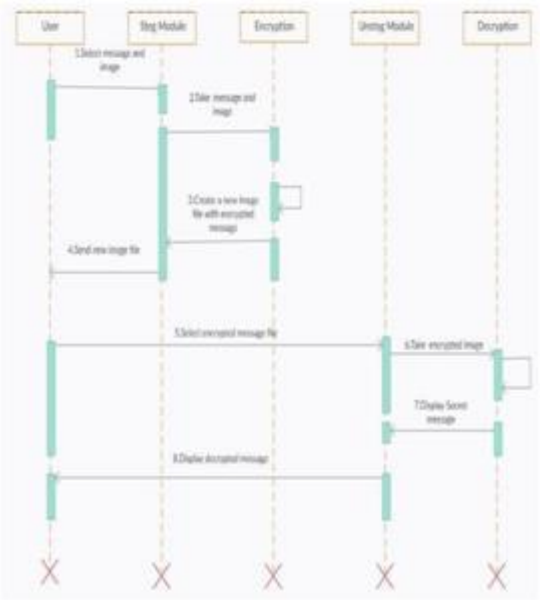


FIG 5. SequenceDiagram.

4. LSB METHOD

In a grey scale image every pel is painted in eight bits. The last bit in a very pel is termed as Least vital bit as its worth can have an effect on the pel worth solely by “1”. So, this property is employed to cover the information within the image. If anyone have thought of last 2 bits as LSB bits as they're going to have an effect on the pel worth solely by “3”. This helps in storing additional knowledge. the smallest amount vital Bit (LSB) steganography is one such technique within which least vital little bit of the image is replaced with knowledge bit. As this technique is at risk of steganalysis thus on create it safer we have a tendency to inscribe the information before embedding it within the image. although the coding method will increase the time quality, however at a similar time provides higher security conjointly. This approach is incredibly easy. during this technique the smallest amount vital bits of some or all of the bytes within a picture is replaced with a bits of the key message. The LSB embedding approach has become the premise of the many techniques that hide messages inside multimedia system carrier knowledge. LSB embedding might even be applied specially knowledge domains.

IV. RESULTS ANDDISCUSSION

The following is the output on implementation of encrypted messages inside valid QR codes.

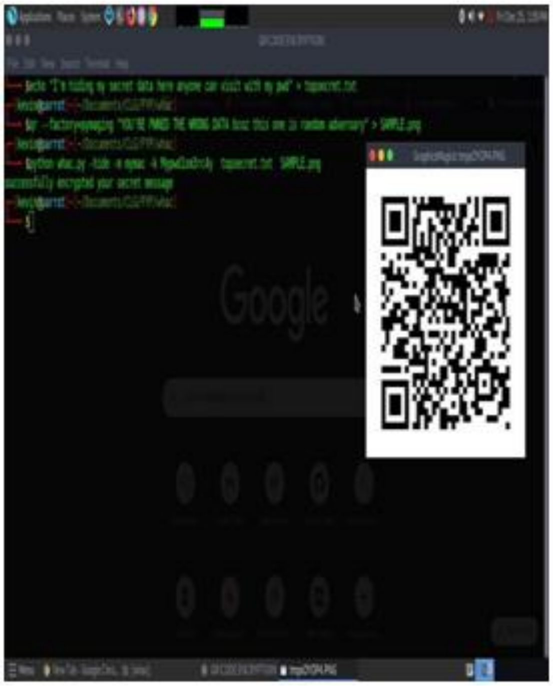
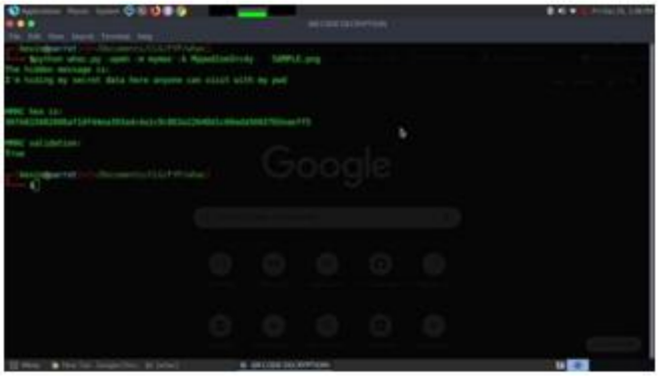

```
└──╼ $echo "I'm hiding my secret data here anyone can [illegible] with my pad" > topsecret.txt
┌─[kevin@parrot]─[~/Documents/[illegible]]
└──╼ $qr --factory=pymaging "YOU'RE [illegible] THE WRONG DATA [illegible] this one is random adversary" > SAMPLE.png
┌─[kevin@parrot]─[~/Documents/[illegible]]
└──╼ $python [illegible].py -hide -m [illegible] -k [illegible] topsecret.txt SAMPLE.png
successfully encrypted your secret message
┌─[kevin@parrot]─[~/Documents/[illegible]]
└──╼ $
```

FIG 6. Encryption.

Figure 6 represents the encryption methods, where that it encodes a message or file so that it can be only read by certainusers.



```
$python whoi.py -open -m mymac -k MypwdIsoStrdy   SAMPLE.png
The hidden message is:
I'm hiding my secret data here anyone can visit with my pwd

HMAC hex is:
[illegible]

HMAC validation:
True
```

FIG 7. Decryption.

Figure 7 represents the decryption method ,it takes encrypted text or other data and converting it back into text you or the computer can read.

FIG 8. Scanning QR code without password.

Figure 8 represents scanning qr code without password, to get the best result, it is desirable that recognizable code.

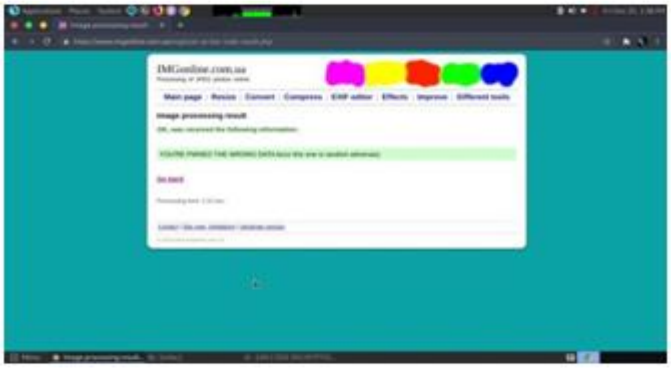


FIG 9. Fake message.

Figure 9 shows the fake message, that gives any presented misleading informations

LSB DECOMPOSITION

There are two necessary parts, cowl image and concealment knowledge, in knowledge concealment technique. the duvet image I is Associate in Nursing 8-bit grey scale image. the dimensions of canopy image is m×n. The concealment knowledge H embedded in I is g-bits bit stream. we tend to use the equation below to precise image C, knowledge D and every constituent on an individual basis. one among the only systems for embedding digital knowledge into a digital cowl is that the Least important Bit technique. take into account Associate in Nursing N×M image during which every constituent worth is pictured by a decimal range within the vary determined by the quantity of bits used. in an exceedingly grey-scale image, with eight bit exactitude per constituent, every constituent assumes a price between [0, 255] and every positive range P. This property permits the decomposition of a picture into a group of binary pictures by separating the into n bit planes.

FIG 10. Generated code.

FIG 11. Ordinary code.

Here that each one the analysis wiped out the paper is applicable to each electronic and written QR codes. Each QR codes may be browse properly to induce constant message, they need constant payload preventive method (generate the QR code then print it), the payload is removable from each QR codes.

V. CONCLUSION

The proposed approach in our project uses a new steganographic approach called QR steganography. The command line tool creates a stegno image in which the personal data is embedded inside the cover file image. Using the LSB along with XTEA-HMAC algorithm in our project for developing the application which is transfer and reliable and compression ratio is moderate compared to other algorithms. Steganographic system that can take advantage of QR codes as containers in which the payload are embedded. Instead of embedding the payload in an image, we embed the payload inside a QR code. The generated QR code has its own message that can be read by any QR reader. A generated QR code is valid i.e it is indistinguishable from any ordinary QR code which makes it a perfect container to hide the payload. Moreover, the message is independent from the payload and it can be used to mislead the adversary. The generated QR codes are tested and the results show that they are indistinguishable from ordinary QR codes. In addition, they are space-efficient, secure compared to other image based steganographic systems, have an acceptable level of noise immunity and they are prone to steganalys is attacks.

VI. ACKNOWLEDGEMENT

We have taken many efforts in this project. However, this project would not be completed without the support and guidance of many individuals. We had a great challenge but a plenty of learning and opportunities to gain huge knowledge on the way writing the report. We express my sincere thanks to **Dr.M.Paulraj**, Principal in Sri Ramakrishna Institute of Technology, Coimbatore for his support and encouragement. Therefore, we would like to take this opportunity to express my profound gratitude and deep regards to the Head of the Department, **Dr.R.M.S.Parvathi**, Professor, CSE and my supervisor, **Ms.D.Betteena Sheryl fernando**, Assistant Professor, CSE for all the time and effort to guide us throughout the whole process. She has been working really hard to help us out with our project, trying her best to clear all our doubts. Besides that, we would like to express our gratitude towards the course coordinator to help us with their knowledge and assist me to complete the project. Finally, we would also like to extend my heartfelt thanks to my dearest parents and family for their unconditional love, encouragement and also support throughout the course.

REFERENCES

[1] MASOUDALAJMI(Member,IEEE),IBRAHIM ELASHRY,HALA S.EL-SAYED AND OSAMA S.FARAGALLAH “Steganography of encrypted messages inside valid QR codes”.in IEE Transactions on image processing,vol.8,pp.2169-3536,06 February2020.

[2] https://www.researchgate.net/publication/339082600_Steganography_of_Encrypted_Messages_Inside_Valid_QR_Codes/fulltext/5e652d 9f92851c7ce053390d/Steganography-of-Encrypted-Messages-Inside-Valid-QR-Codes.

[3] Arun Kumar Singh, Juhi Singh, Steganography in Images Using LSB Technique, International Journal of Latest Trends in Engineering and Technology (IJLTET). Alturki.F.T.,Almutairi.A.F.andMersereauu.R.

[4] M. (2007), “Analysis of blind data hiding using discrete cosine transform phase modulation”, Signal Processing: Image Communication 22, 347-362.

[5] Al-Qershi. O. M. and Khoo. B. E. (2011) “High capacity data hiding schemes for medical images based on difference expansion” The Journal of Systems and Software 84,105-112.

[6] Ballesteros. D. M. L and Moreno. J. M. A. (2012) “Highly transparent steganography model of speech signals using Efficient Wavelet Masking”, Expert Systems with Applications 39,9141-9149.

[7] Rathika R, Prof.S.Kumaresan (2016), Survey on Reversible Data Hiding Techniques, International Conference on Advanced Computing and Communication Systems (ICACCS),Coimbatore

[8] Princy Raj, Sreekumar K, A Survey on Reversible Data Hiding in Encrypted Image, (IJCSIT) International Journal of Computer Science and InformationTechnologies(2014).

[9] Shweta Patil, S. S Katariya , Data Hiding Techniques: A Review, International Journal of Computer Applications(2015).

[10] Sukhdeep Kaur, Manshi Shukla, Reversible Data Hiding and its Methods: A Survey, International Journal of Computer Science and Mobile Computing, pp 821-826(2014).

[11] Xinpeng Zhang, Zhenxing Qian, Guorui Feng, Yanli Ren, Efficient reversible data hiding in encrypted images, Journal of Visual Communication and Image Representation(2014).

[12] Wien Hong, Tung-Shou Chen, Han-Yan Wu, An Improved Reversible Data Hiding in Encrypted Images Using Side Match, IEEE Signal Processing Letters(2012).

[13] Jiang Yu, Wen Si, Fenyong Li ,Reversible data hiding in encrypted messages with auxiliary syndrome, international symposium on intelligent signal processing and communication systems, Xiamen, china(2017).

[14] S. Gueron, S. Johnson, and J. Walker, ‘‘SHA- 512/256,’’ in Proc. 8th Int. Conf. Inf. Technol., Generat., Apr. 2011, pp. 354–358.

[15] S.Li,G.Chen,andX.Zheng,‘‘Chaos-based encryption for digital images and videos,’’ in Multimedia Security Handbook, no. 4, B. Furht and D. Kirovski, Eds. Boca Raton, FL, USA: CRC Press, 2004, pp.133–167.

[16] K. Sahu and G. Swain, ‘‘Dual stego-imaging based reversible data hiding using improved LSB matching,’’Int. J. Intell. Eng. Syst., vol. 12, no. 5,pp. 63–73, Sep.2019.K. K. Smith, ‘‘Dynamic variable-length error correction code,’’ U.S. Patent 6961890.Nov. 1, 2005. [29] H. Wang and S. Wang, ‘‘Cyber warfare: Steganography vs. steganalysis,’’ Communication ACM, vol. 47, no. 10, pp. 76–82, Oct. 2004.

[17] S.Manoharan,‘‘An empirical analysis of steganalysis,’’inProc.3rdInt. Conf. Internet Monitor. Protection, Jun.2008, pp. 172–17.