QR BASED DATA HIDING IN ENCRYPTED IMAGE BASED ON MULTI-SECRET SHARING AND LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHM

Senthil Balaji[1] V,Abarna[2] J, Lakshmi Rathnaa[3] M
[1]*Assistant Professor, Information Technology, Saranathan College Of Engineering, Trichy*
[2,3]*Information Technology, Saranathan College Of Engineering,Trichy*

Abstract- **Information/data hiding is a mechanism which ensures that the presence of the secret data remains undetected. Two types of data hiding techniques are most popular, they are cryptography and steganography. Where cryptography is science of writing secret code and steganography is art and science of hiding the secret code. In cryptography data is converted to unreadable form, so that unauthorized users cannot access the secret data. Steganography process hides message into cover file and forms a stego file. In image steganography there is a need of method which will increase the security, reduce the distortion in the stego file and recovers the data without any loss. In the era of multimedia and internet there is need of reducing time for transmission. The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. The secret text was hidden within the QR image. Then QR image can be hidden within secret image. The secret image can be obtained by super imposing the two shares. Conventional k out of n visual cryptography scheme is used to encrypt a single image into n shares. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. A text is written and hidden inside an image. LSB method is used for this purpose. Now the image is splitted into shares. Each share is encrypted using XOR method. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. At the receiver end, the hidden data is extracted from the recovered image.**

Index Terms- **Data Hiding, Image Privacy, Encryption, Multi-Secret Sharing, Security**

I. INTRODUCTION

BACKGROUND

Steganography is the practice of hiding secret messages (hidden text) within every day, seemingly innocuous objects (cover text) to produce a stegno text. The recipient of a stegno text can use his knowledge of the particular method of steganography employed to recover the hidden text from the stegno text. The goal of steganography is to allow parties to converse covertly in such a way that an attacker cannot tell whether or not there is hidden meaning to their conversation. This sets steganography apart from cryptography which, although providing for private communication, can arouse suspicion based solely on the fact that it is being used. Modern steganography was characterized by G J Simmons when he stated the problem in terms of prisoners attempting to communicate covertly in the presence of a warden. Alice and Bob, prisoners, are allowed to communicate, but their channel is through the warden, Ward. Alice wishes to pass secret messages to Bob in such a way that Ward can determine neither the contents of the secret messages, nor even that secret messages are being passed. In modern times, this problem can be observed in national intelligence agencies attempting to detect public yet covert communication between terrorists, or communication between citizens in oppressive states which have outlawed cryptography.

STEGANOGRAPHY WORKING PROCESS

Steganography replaces inessential or
unused bits in regular pc files (Graphics, sound, text) with bits of different and invisible info. Hidden information is the other regular computer file or encrypted information.Steganography differs

from cryptography in an approach that it masks the existence of the messageWherever cryptography works to mask the content of the message.Steganography generally utilized in conjunction with encoding. Associate in nursing encrypted file should hide info victimisation steganography, thus albeit the encrypted file is deciphered, the hidden information is not seen.

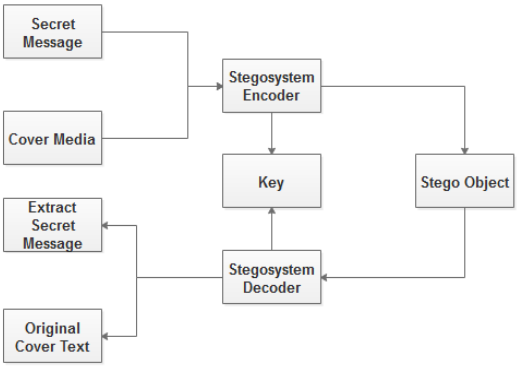


Fig 1.1 Processing steps for Steganography

II. TYPES OF STEGANOGRAPHY

There are other ways to cover the message in another, standard are Least important bytes and Injection. Once a file or a picture is formed there are few bytes within the file or image that aren't necessary or least necessary. These style of bytes may be replaced with a message while not damaging or substitution of the initial message, by that the secrete message is hidden within the file or image. Another way could be a message may be directly injected into a file or image. However dur-ing this approach the scale of the file would be in-creasing consequently reckoning on the secrete message

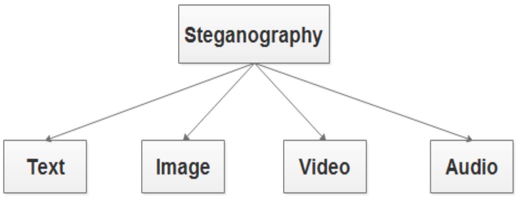


Fig 1.2: Types of Steganography

STEGANOGRAPHY IN IMAGE

Digital pictures area unit the foremost wide used cowl objects for steganography.Thanks to the provision numerous of varies of assorted file formats for various applications the algorithmic rule used for these formats differs consequently.

An image is assortment of bytes (know as pixels for images) containing totally different light-weight intensities in numerous areas of the image.Once managing digital pictures to be used with Steganography, 8-bit and 24-bit per component image files area unit typical. Each have blessings and drawbacks 8-bit pictures area unit a good format to use attributable to their comparatively tiny size. The disadvantage is that solely 256 attainable colours will be used which might be a possible downside throughout encryption.

Typically a grey scale color palette is employed once managing 8-bit pictures like (.GIF) as a result of its gradual modification in color would be tougher to discover once the image has been encoded with the key message. 24-bit pictures supply way more flexibility once used for Steganography. The massive numbers of colours (over sixteen million) that may be used go well on the far side the human sensory system , that makes it terribly exhausting to discover once a secret message, has been encoded,Great deal of knowledge will be encoded in to 24-bit pictures because it is compared to 8-bit pictures. The disadvantage of 24-bit digital pictures is their size that is extremely high and this makes them suspicious our web because of their significant size in comparison to 8-bit pictures. Reckoning on the sort of message and kind of the image totally different algorithms area unit used.

Few types in Steganography in Images:

Least significant bit insertion

Masking and filtering

Redundant Pattern Encoding

Encrypt and Scatter

Algorithms and transformations

Least significant bit insertion

Least significant Bit (LSB) insertion is most generally proverbial rule for image steganography, it involves the modification of LSB layer of image. During this technique, the message is hold on within the LSB of the pixels that can be thought-about as random noise. Thus, fixing them doesn't have any obvious impact to the image.

Masking and filtering

Masking and filtering techniques work higher with twenty four bit and gray scale pictures. They hide data in a very method the same as watermarks on actual paper and square measure typically used as digital watermarks. Masking the pictures changes the pictures build to confirm that changes cannot be detected make the changes in multiple little proportions. Compared to LSB masking is additional sturdy and disguised pictures passes cropping, compression and a few image process. Masking techniques introduce info in important areas in order that the hidden message is additional integral to the quilt image than simply concealing it within the "noise" level. This makes it additional appropriate than LSB with, as an example, lossy JPEG pictures.

Redundant Pattern coding

Redundant pattern coding is to some extent the same as unfold spectrum technique. During this technique, the message is scattered throughout the image supported rule. This method makes the image ineffective for cropping and rotation. Multiple smaller pictures with redundancy increase the prospect of sick even once the stegano-image is manipulated.

Encrypt and Scatter

Encrypt and Scatter techniques hides the message as dissonance and dissonance Storm is an example that uses employs unfold spectrum and frequency hopping. Previous window size and information channel are wont to generate a random range and inside this random range, on all the eight channels message is scattered throughout the message. Every channel rotates, Swaps and interlaces with each alternative channel. Single channel represents one bit and as a result there are several unaffected bits in every channel. During this technique it's terribly complicated to extend the particular message from stegano-image. This system is safer compared to LSB because it wants each rule and key to rewrite the bit message from stegano-image. Some users like this technique for its security because it wants each rule and key despite the stegano image. This technique like LSB lets image degradation in terms of image process, and compression.

Algorithms and transformations

LSB modification technique for pictures will hold smart if any reasonably compression is finished on the resultant stego-image e.g. JPEG, GIF. JPEG pictures use the separate cos remodel to attain compression. DCT could be a lossy compression remodel as a result of the cos values can't be calculated precisely, and recurrent calculations mistreatment restricted preciseness numbers introduce misreckoning errors into the ultimate result. Variances between original information values and fixed information values depend upon the tactic wont to calculate DCT.

The area differs in what feature of the steganography is used in every system.

1. Confidential communication and secret knowledge storing.

The "secrecy" of the embedded knowledge is important during this space.

Historically, steganography are self-addressed during this space. Steganography provides United States with:

(A) Potential capability to cover the existence of confidential knowledge.
(B) Hardness of police work the hidden (i.e., embedded) knowledge
(C) Enhancing the secrecy of the encrypted knowledge.

In apply, once you use some steganography, you need to first choose a vessel information in line with the dimensions of the embedding information. The vessel ought to be innocuous. Then, you engraft the confidential information by exploitation associate embedding program (which is one element of the steganography software) in conjunction with some key. Once extracting, you (or your party) use associate extracting program (another component) to revive the embedded information by a similar key ("common key" in terms of cryptography). During this case you wish a "key negotiation" along with your party before you begin confidential communication. Attaching a stego file to associate e-mail message is another example during this application space. However you and your party should do a "sending-and-receiving" action that would be noticed by a 3rd party. So, e-mailing isn't a totally secret communication technique.

Protection of data alteration

We benefit of the fragility of the embedded information during this application space. We declared within the Home Page that "the embedded information will well be fragile than be terribly strong." Actually, embedded information is fragile in most steganography programs. Especially Qtech Hide & read program embeds information in an especially fragile manner. However, this fragility opens a brand new direction toward associate degree information-alteration protecting system like a "Digital Certificate Document System." the foremost novel purpose among others is that "no authentication bureau is required." If it's enforced, individuals will send their "digital certificate data" to anyplace within the world through web. Nobody will forge, alter, nor tamper such certificate information. If forged, altered, or tampered, it's simply detected by the extraction program.

Access control system for digital content distribution

In this area embedded information is "hidden", however is "explained" to publicize the content.

Today, digital contents are becoming additional and additional normally distributed over net than before. As an example, music firms unharness new albums on their Webpage in a very free or charged manner. However, during this case, all the contents square measure equally distributed to those who will build access to the page. So, a normal net distribution theme isn't fitted to a "case-by-case" and "selective" distribution. After all it invariably potential to connect digital contents to e-mail messages and send them to the purchasers. However it'll takes heaps of value in time.If you have got some valuable content, that you think that it's distributable if somebody extremely desires it, and if it's potential to transfer that content on net in some covert manner. And if you'll be able to issue a special "access key" to extract the content by selection, you may be terribly happy regarding it. A stegnographic theme will facilitate notice this kind of system.

Media Database systems

We have developed a model of AN "Access management System" for digital content distribution through web. The subsequent steps justify the theme.
(1) A content owner classify his/her digital contents in a very folder-by-folder manner, and enter the total folders in some massive vessel in keeping with a steganographic technique victimization folder access keys, and transfer the embedded vessel (stego data) on his/her own Webpage.
(2) Thereon Webpage the owner explains the contents exhaustive and publicize worldwide. The contact data to the owner (post mail address, e-mail address, sign, etc.) are announce there.
(3) The owner might receive an access-request from a client World Health Organization watched that Webpage. Therein case, the owner might (or might not) creates an access key and supply it to the client (free or charged).
In this mechanism the foremost necessary purpose is, a "selective extraction" is feasible or not.

In this application space of steganography secrecy isn't necessary, however unifying 2 kinds of knowledge into one is that the most vital.
Media knowledge (photo image, movie, music, etc.) have some association with alternative data. A photograph image, for example, could have the subsequent.
(1) The title of the image and a few object data.
(2) The date and therefore the time once the image was taken.
(3) The camera and therefore the photographer's data.
Formerly, these are annotated beside the every image within the album.

Recently, the majority cameras square measure digitalized. They're low-cost in worth, straightforward to use, fast to shoot. They eventually created folks feel reluctant to figure on expansion every image. Now, most home PC's square measure cursed the massive quantity of picture files. During this state of affairs it's terribly laborious to search out a selected shot within the piles of images.Once you wish to search out a selected image, you'll build an enquiry by keywords for the target image. However, the annotation knowledge in such package aren't unified with the target footage. Every annotation solely contains a link to the image. Therefore, once you transfer the images to a special album package, all the annotation knowledge square measure lost.

This drawback is technically remarked as "Metadata (e.g., annotation knowledge) during a media information system (a picture album software) square measure separated from the media data (photo data) within the information managing system (DBMS)." this is often an enormous drawback.

Steganography will solve this drawback as a result of a steganography program unifies 2 forms of information into one by approach of embedding operation. So, information will simply be transferred from one system to a different while not hitch. Specifically, you'll be able to enter all of your good/bad memory (of your sight-seeing trip) in every snap shot of the digital icon. you'll be able to either send the embedded image to your friend to extract your memory on his/her computer, otherwise you could keep it silent in your own computer to get pleasure from extracting the memory 10 years when If a "motion image steganography system" has been developed within the close to future, a keyword primarily based movie-scene retrieving system are going to be enforced. It'll be a step to a "semantic motion picture retrieval system."The importance of information activity techniques comes from the very fact that there's no responsible over the medium through that the data is send, in alternative words the medium isn't secured. So, some strategies area unit required in order that it becomes troublesome for causeless user to extract the data from the message. Few reasons behind information activity are: Personal and personal information, Sensitive information, Confidential data and trade secret ,to avoid misuse of data. Unintentional damage to data, human error and accidental deletion of data , Monetary and blackmail purposes ,To hide traces of crime.

III. USES OF STEGANOGRAPHY

Steganography is an answer that makes it potential to send news and knowledge while not being censored and while not their worry of the messages being intercepted and half-tracked back to USA. It's additionally potential to easily use Steganography to store data on a location. As an example, many data supply like our non-public banking data and a few military secrets is hold on during a cowl source. Steganography can even be wont to implement watermarking. There areas unit many steganographic techniques that area unit being employed to store watermarks in knowledge. The most distinction is that the aim of steganography is concealment data and watermarking is simply extending the quilt supply with additional data. Since folks won't settle for noticeable changes in pictures, audio or video files thanks to a watermark, steganographic ways is wont to hide this. E-commerce permits for a motivating use of Steganography. In current e-commerce transactions, most of the users area unit protected by a username and positive identification, with no real technique of verification that the user is that the actual card holder.

Cryptography

Cryptography is that the science of exploitation arithmetic to cypher and decode information. Cryptography permits you to store sensitive info or transmit it across insecure networks (like the Internet) so it cannot be scan by anyone except the supposed recipient.While cryptography is that the science of securing information, cryptology is that the science of analyzing and breaking secure communication. Classical cryptology involves a noteworthy combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts also are known as attackers. Cryptology embraces each cryptography and cryptology.

Cryptography is employed in several applications like banking transactions cards, pc passwords, and e- commerce transactions.
Three varieties of cryptanalytic techniques employed in general.
1. Symmetric-key cryptography
2. Hash functions.
3. Public-key cryptography

Symmetric-key Cryptography:

Both the sender and receiver share one key. The sender uses this key to cypher plaintext and send the cipher text to the receiver. On the opposite facet the receiver applies an equivalent key to decipher the message and recover the plaintext.

With interchangeable cryptography, an equivalent key's used for each coding and cryptography. A sender and a recipient should have already got a shared key that's well-known to each. Key distribution may be a tough drawback and was the impetus for developing uneven cryptography. With uneven crypto, 2 completely different keys are used for coding and cryptography. Each user in associate uneven cryptosystem has each a public key and a personal key. The personal key's unbroken secret in any respect times, however the general public key is also freely distributed. Data encrypted with a public key might solely be decrypted with the corresponding personal key. So, causation a message to John needs encrypting that message with John's public key. Solely John will decipher the message, as solely John has his personal key. Any information encrypted with a personal key will solely be decrypted with the corresponding public key. Similarly, Jane may digitally sign a message together with her personal key, and anyone with Jane's public key may decipher the signed message and verify that it absolutely was really Jane World Health Organization sent it. Symmetric is mostly in no time and ideal for encrypting giant amounts of information (e.g., a complete disk partition or database). Uneven is way slower and might solely write items of information that square measure smaller than the key size (typically 2048 bits or smaller). Thus, uneven crypto is mostly accustomed write parallel coding keys that square measure then accustomed write a lot of larger blocks of information. For digital signatures, uneven crypto is mostly accustomed write the hashes of messages instead of entire messages.

A cryptosystem provides for managing cryptological keys as well as generation, exchange, storage, use, revocation, and replacement of the keys.

Public-Key Cryptography: This is the foremost revolutionary thought within the last 300-400 years. In Public-Key Cryptography 2 connected keys (public and personal key) are used. Public key is also freely distributed, whereas it paired personal key, remains a secret.The general public key used for encoding and for decipherment personal key used.

Public-key cryptography, or uneven cryptography, is an encoding theme that uses 2 mathematically connected, however not identical, keys - a public key and a non-public key. Not like bilateral key algorithms that consider one key to each cypher and decipher, every key performs a novel operate. The general public key won't to cypher and also the personal key's wont to decipher. It is computationally impossible to reason the personal key supported the general public key. attributable to this, public keys are often freely shared, permitting users a simple and convenient technique for encrypting content and collateral digital signatures, and personal keys are often unbroken secret, making certain solely the homeowners of the personal keys will decipher content and make digital signatures.

Since public keys got to be shared however are too massive to be simply remembered, they're hold on digital certificates for secure transport and sharing. Since personal keys don't seem to be shared, they're merely hold on within the computer code or software system you utilize, or on hardware (e.g., USB token, hardware security module) containing drivers that permit it to be used along with your computer code or software system.

Hash Functions: No secret's employed in this algorithmic rule. A fixed-length hash worth is computed as per the plain text that produces it not possible for the contents of the plain text to be recovered. Hash functions are utilized by several operational systems to encipher passwords.

2. STEPS FOR QR BASED DATA HIDING IN ENCRYPTED IMAGE

QR code generation

Sender need to type the secret message(Message text) which is sent to the receiver.Message text is present in the form of normal text in English words. Sender can type any number of words. QR code converter is used to generate QR code for that given secret message.the secret message is in the form of QR code.

Select cover image to upload and hiding

The sender choose the image for information hiding.Here image is used as a cover media for the secret message. The image will be in any extension.After choosing the cover image QR code will be hidden within cover image.For hiding process we are using Multi Pixel Value Differencing technique (MPVD) with LSB approach.

Splitting Stegno image and Encryption

The cover image will be divided into “n” number of shares. “n” is the product of rows and columns. Here we are splitting the stegno image into 16 shares using matrix method.For encryption process we are using XOR based encryption.Each share is encrypted by using XOR encryption algorithm.XOR encryption requires that both encryptor and decryptor have access to the encryption key.

Multi Secret Sending

The encrypted shares can send to multiple receivers.By using this module, all the encrypted shares will be sent to the receiver in a single transmission.This will save time.

Decryption

Receiver will receive all the encrypted shares in a single transmission.Each received share will be decrypted individually using inverse XOR method.The output of this module will be an individual share in the decrypted form.All the decrypted individual shares are the input for this module.These individual shares will be joined together to form the original (secret) image.

Extraction of QR code and secret message

In this module receiver can retrieve QR code and text.After decryption image shares receiver can extract QR based text.The recovered image can be viewed as a complete single image.Then text will be recovered from the image using secret key.

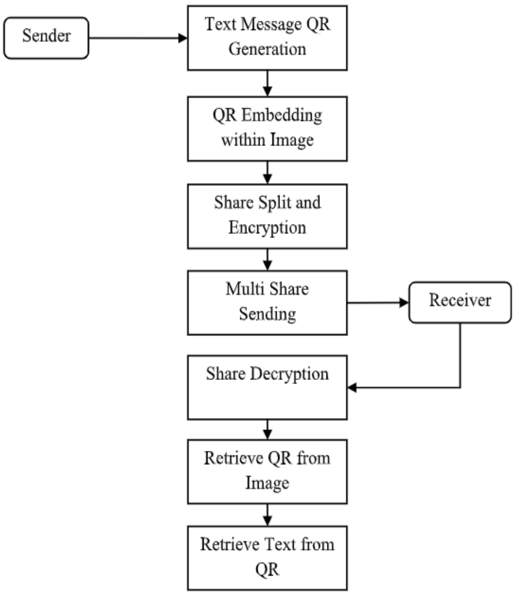
3. EXISTING SYSTEM

In this system we introduce a new class of reversible data hiding in encrypted images.The image provider has a shared secret key with the receiver. If anyone who knows the embedding procedure can hide.The Paillier-based technique can perform encryption for each pixel.Security will be weak when stream-cipher-based schemes are used. The proposed scheme is at least a candidate to preserve both of efficiency and security. This system provide addition homomorphism in multi-secret sharing (OAMSS). k out of n multi secret sharing scheme is used to convert a single image into n shares.OR based encryption scheme implement to encrypt the shares.Divide the original image into smooth area and coarse area, and embed several least significant bit (LSB) planes of the RDH method.The image provider shares a secret key with the receiver, and the data hider can embed a secret message without any knowledge of this key. Existing systemdoes not support multiple secret sharing in a single transmission.It applicable only for JPEG images. In existing system creates meaningless shares. Those meaningless share initiates the intruder to try and decrypt the shares. In OR based Encryption the file Size may get vary.

IV. PROPOSED SYSTEM

Information security is major concern today because day by day number internet users are increasing so secret information is shared for every seconds around the world side by side number of intruders also increasing. In order to avoid this ,additional security will be provided for confidential data transmission. Sender input a text to convert into QR and select cover image to share.The QR image was hidden into the cover image using MPVD with LSB to improve security.A secret stegno image is converted to n shares of images.Each share is then encrypted by using XOR encryption.XOR based visual cryptography is used to recover the secret image perfectly.Multi secret sharing is used to send more than one image in a single transmission.The secret image and the recovered image will be of the same size.Multi secret sharing is used to send multiple shares at the same time. We enhances security with XOR algorithm.

V. SYSTEM ARCHITECTURE



VI. MODULES

6.1 Text Hidden into QR code

Sender will generate the content for transmit to the receiver.Message can present in the form of normal text in English words. QR code generator will generate QR code for secret message.

6.2Image Upload and Hiding

This process is to select cover media for information hiding.Here images are used as a cover media for the secret message. The QR image will be hidden within cover image using MPVD with LSB approach.

6.3Share Split and Encryption

The cover image will be divided into "n" number of shares."n" is the product of rows and columns.Each share is encrypted using XOR encryption.XOR encryption requires that both encryptor and decryptor have access to the encryption key.

6.4 Multi Secret Sending

After share split and encryption ,all the individual encrypted shares will be stored in a folder of sender system. In a single transmission all the encrypted shares will be sent to the receiver by using this module. Because of single transmission will save time for the user.

6.5 share decryption

After multi secret sending , all the encrypted shares will be received by the receiver in a single transmission.Each received share will be decrypted individually using inverse XOR method which is the advanced technology.The output of this module will be an individual share in the decrypted form.All the decrypted individual shares are the input for this module. Original image can be obtained by joining these individual decrypted shares.

6.6 Recovered QR code and Text Extracting

This is the finial module where the receiver can retrieve QR code and text after transmission.After decryption process on image shares receiver can extract exact QR based text.The recovered image can be viewed as a complete single image without loss of any shares.Then text will be recovered from the image using key(secret key).

VII. PSEUDOCODE

Step1: Get the text from the sender which is converted into QR code.

Step2: Select the cover image and hide the QR code into the cover image.

Step3: Split the stegno image into multiple shares

Step4: Encrypt the each and every shares.

Step5: Sent all the encrypted shares and secret key to the receiver in a single transmission.

Step6: Get the secret message after decryption and reconstruction process.

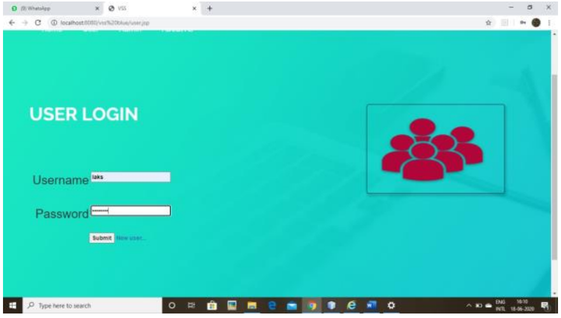
VIII. IMPLEMENTATION

8.1 Text Hidden into QR code

Text hiding is a process of embedding the secret text imperceptibly into the cover media by minimally modifying the elements of the cover media.

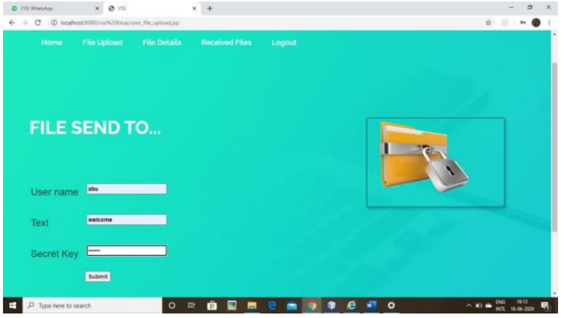
In this module sender will generate content for transmit to the receiver. Message text is present in the form of normal text in English words. Uploaded texts message was converted into QR format

.


USER LOGIN

Username laks

Password ••••••••

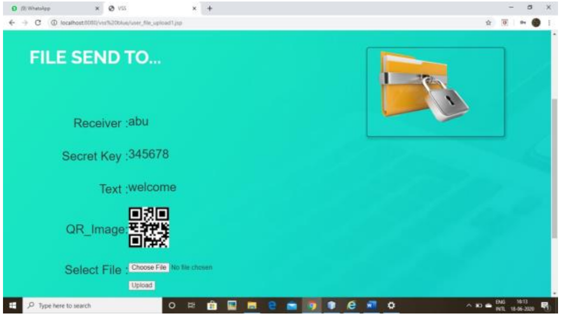


FILE SEND TO...

User name abu

Text welcome

Secret Key ••••••


FILE SEND TO...

Receiver :abu

Secret Key :345678

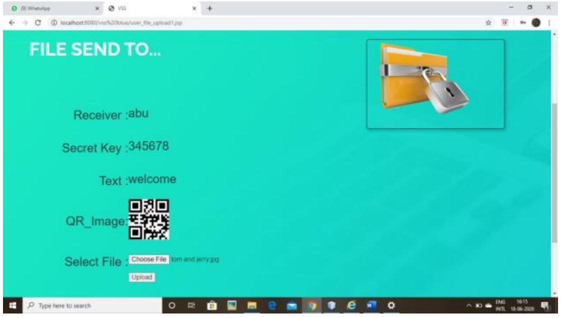
Text :welcome

QR_Image

Select File : Choose File No file chosen

8.2 Image Upload and Hiding

This process is to select cover media for information hiding. Here images are used as a cover media for the secret message. Cover image is also select by the sender when create the secret message. Original message is hidden into the cover media (image) to improve the security of data sharing. The steganographed image that has to sent should be uploaded. The image should be any one of the image supporting formats. A text is written and hidden inside a secret image. This is done by using LSB method. The cover image is called as a steganographed image.


FILE SEND TO...

Receiver :abu

Secret Key :345678

Text :welcome

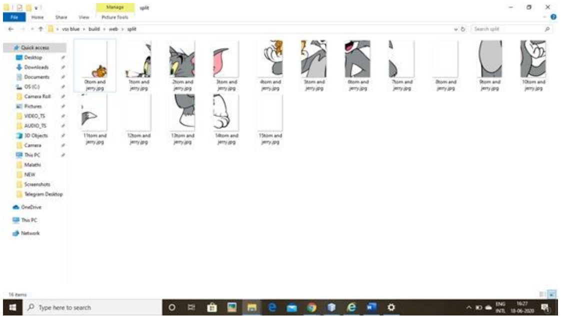
QR_Image

Select File : Choose File tom and jerry.jpg

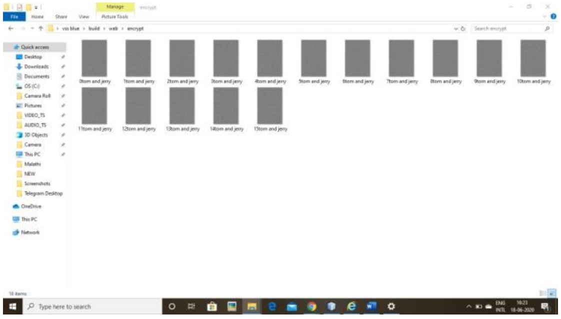
8.3 Share Split and Encryption

The uploaded image will be divided into "n" number of shares according to the user requirements. "n" is the product of rows and columns. Here, in this project, the number of shares is 16 (4*4). Maximum number of shares is fixed to 8 * 8. Splited image shares will be encrypted separately using XOR method. A key is used to encrypt the shares. Exclusive-or encryption requires that both encryptor and decryptor have access to the encryption key, but the encryption algorithm, while extremely simple, is nearly unbreakable. That key will be mailed to the receiver. If JPEG image is used, the encrypted share will be in black and white color. It will look like a QR code.

Share split :

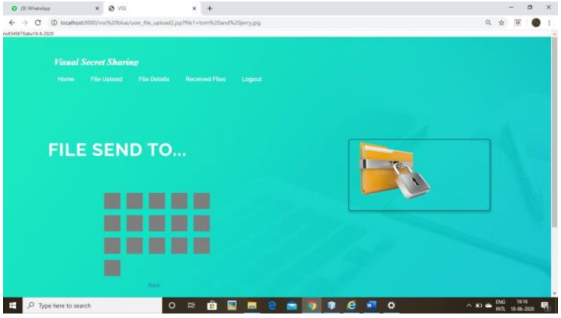


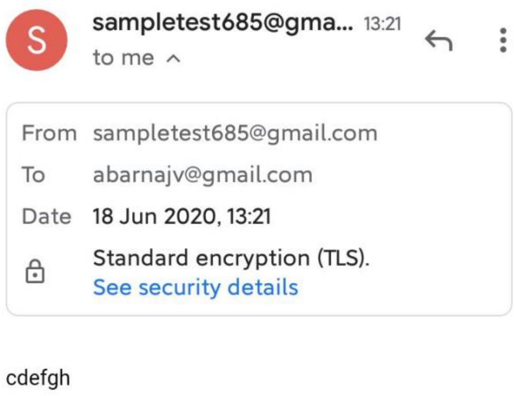
Share Encryption :



8.4 Multi Share Sending

All the individual encrypted shares will be stored in a folder. By using this module, all the encrypted shares will be sent to the receiver in a single transmission. This single transmission enables receiver to receive all the shares at a time. This will helps to avoid the information or share missing and also it saves transmission and receiving time for both sender and receiver.





sampletest685@gma... 13:21

to me

From sampletest685@gmail.com

To abarnajv@gmail.com

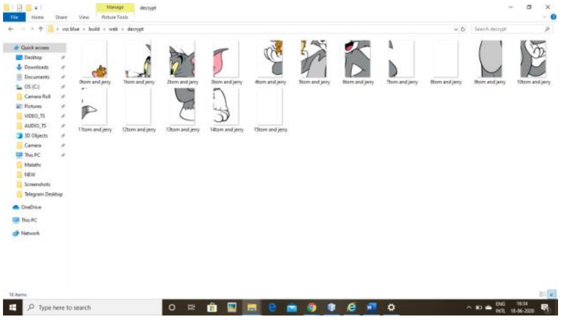
Date 18 Jun 2020, 13:21

Standard encryption (TLS).
See security details

cdefgh

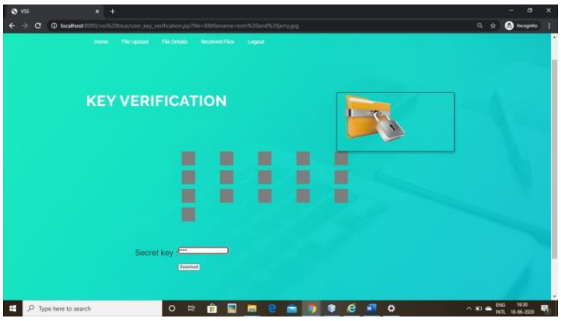
8.5 Image Decryption

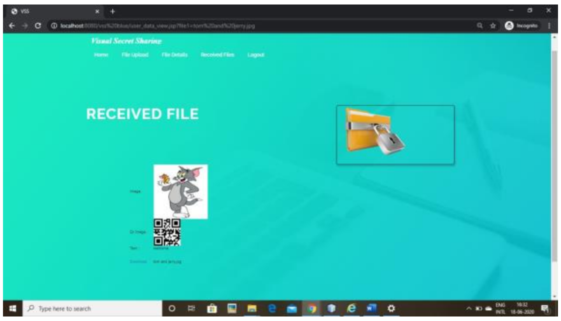
All the encrypted shares will be received by the receiver in a single transmission. Each received share will be decrypted individually using inverse XOR method. The key that is received through mail is used in this decryption process. Private key is used for both encryption and decryption process. The output of this module will be an individual share in the decrypted form. All the decrypted individual shares are the input for this module. These individual shares will be joined together to form the original (secret) image. The recovered image can be viewed as a complete single image. The dimensions of both the original image and the recovered image will be the same.



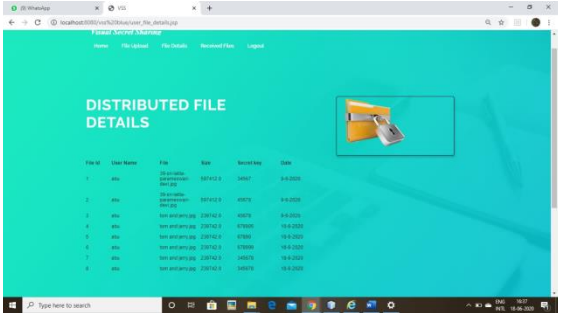
8.6 Recovered QR code and Text Extracting

In this module receiver can retrieve QR code and text. After decryption image shares receiver can extract QR based text. Data extraction is the process of extracting the original data. The hidden text will be recovered from the secret image. Receiver gets the secret message with cover text. LSB method is used to retrieve the hidden text Specific key is generated and shared to the receiver during the process of message sending. Receiver can decrypt the text using shared secret key. Then the original message is shown to the receiver.





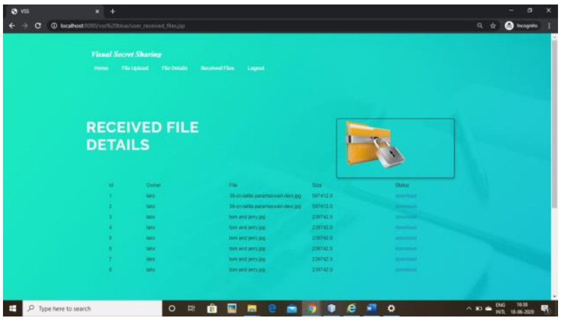
Sender File Details :



DISTRIBUTED FILE DETAILS

File Id	User Name	File	Size	Secret key	Date
1	abu	39-sri-lalita-parameswari-devi.jpg	597412.0	34567	8-6-2020
2	abu	39-sri-lalita-parameswari-devi.jpg	597412.0	45678	8-6-2020
3	abu	tom and jerry.jpg	239742.0	45678	8-6-2020
4	abu	tom and jerry.jpg	239742.0	678906	18-6-2020
5	abu	tom and jerry.jpg	239742.0	67890	18-6-2020
6	abu	tom and jerry.jpg	239742.0	678999	18-6-2020
7	abu	tom and jerry.jpg	239742.0	345678	18-6-2020
8	abu	tom and jerry.jpg	239742.0	345678	18-6-2020

Receiver File Details :



RECEIVED FILE DETAILS

Id	Owner	File	Size	Status
1	laks	39-sri-lalita-parameswari-devi.jpg	597412.0	download
2	laks	39-sri-lalita-parameswari-devi.jpg	597412.0	download
3	laks	tom and jerry.jpg	239742.0	download
4	laks	tom and jerry.jpg	239742.0	download
5	laks	tom and jerry.jpg	239742.0	download
6	laks	tom and jerry.jpg	239742.0	download
7	laks	tom and jerry.jpg	239742.0	download
8	laks	tom and jerry.jpg	239742.0	download

IX. CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. In this work, a text message was hidden within QR Code then the QR will be hidden within image. The sender has to create text and generate QR for input text then select the image to hide the QR image using MPVD with LSB approach that should be sent the message secretly to the receiver. Then the secret image is splitted into "n" number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image.

REFERENCES

1. Bartwal, Monika, and Rajendra Bharti. &quot;Lossless and Reversible Data Hiding in Encrypted Images With Public Key Cryptography.&quot; Annals of Computer Science and InformationSystems 10 (2017): 127-134.

2. Cao, Xiaochun, Ling Du, Xingxing Wei, Dan Meng, and Xiaojie Guo. &quot;High capacityreversible data hiding in encrypted images by patch-level sparse representation.&quot; IEEEtransactions on cybernetics 46, no. 5 (2015): 1132-1143.

3. Chuman, Tatsuya, Kenta Iida, and Hitoshi Kiya. &quot;Image manipulation on social media forencryption-then-compression systems.&quot; In 2017 Asia-Pacific Signal and InformationProcessing Association Annual Summit and Conference (APSIPA ASC), pp. 858-863. IEEE,2017.

4. Chuman, Tatsuya, Kenta Kurihara, and Hitoshi Kiya.&quot;On the security of block scrambling-based etc systems against extended jigsaw puzzle solver attacks.&quot; IEICE TRANSACTIONS on Information and Systems 101, no. 1 (2018): 37-44.

5. Dragoi, Ioan Catalin, Henri-George Coanda, and Dinu Coltuc.&quot;Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction.&quot;In 2017 25th European Signal Processing Conference (EUSIPCO), pp. 2186-2190. IEEE,2017.

6. Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi. &quot;New framework for reversible data hiding in encrypted domain.&quot; IEEE Transactions on Information Forensics and Security 11,no. 12 (2016): 2777-2789.

7. Kobayashi, Hiroyuki, and Hitoshi Kiya. &quot;Bitstream-Based JPEG Image Encryption with File-Size Preserving.&quot; In 2018 IEEE 7th Global Conference on Consumer Electronics(GCCE), pp. 384-387. IEEE, 2018.

8. Kurihara, Kenta, Masanori Kikuchi, Shoko Imaizumi, Sayaka Shiota, and Hitoshi Kiya.&quot;An encryption-then-compression system for jpeg/motion jpe standard.&quot; IEICE Transactions

on Fundamentals of Electronics, Communications and Computer Sciences 98, no. 11 (2015):2238-2245.

9. Qian, Zhenxing, Hang Zhou, Xinpeng Zhang, and Weiming Zhang. &quot;Separable reversible-data hiding in encrypted JPEG bitstreams.&quot;

IEEE Transactions on Dependable and Secure Computing 15, no. 6 (2016): 1055-1067.

10. Xiang, Shijun, and Xinrong Luo. &quot;Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group.&quot; IEEE Transactions on Circuits and Systems for Video Technology 28, no. 11 (2017): 3099-3110.

11. Yi, Shuang, and Yicong Zhou. &quot;Binary-block embedding for reversible data hiding in encrypted images.&quot; Signal Processing 133 (2017): 40-51.

12. Zhou, Jiantao, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang.&quot;Secure reversible image data hiding over encrypted domain via key modulation.&quot; IEEE transactions on circuits and systems for video technology 26, no. 3 (2015): 441-452.