ABSTRACT

With the increasing application of image processing techniques in various areas, contrast techniques in digital image processing systems concepts. Unsharp image masking is the one of the efficient approach technique in among the availability of image compression methods, which could give satisfactory results. However, accurately setting the unsharp masking algorithmic parameters is a difficult task. In this paper, random number generation phases made the image in unrecognized format. The property of this entitled is to increase the security levels of the encrypted encoded image. Here one key is needed to encrypt and decrypts the image, and then we had to applied compression techniques for a better compression and to prepare unrecognized and unreadable format. Finally, the Experiments are conducted to demonstrate the feasibility of the security is providing to the image in network security.

Keywords: - Raw Images, Image Encryption Technique, decryption technique, Compression techniques and Random key.

1. INTRODUCTION

The term cryptography is information security and the processes of writing / reading secret messages / code. This term cryptography is way to conceal the information in storage. It is personally related to restraints of cryptology and cryptanalysis. Here we will try to learn the basics of cryptography. Simply technique to encode the information or code into unreadable format. Computer security has to reinvent itself. New technologies and new applications bring new threats. Above all with the growth of data a communication cryptography and data security are the necessary requirements for communication isolation. The entitled “Image Masking and Compression Using Random Number Generation” of this paper is to increase the security levels of the encrypted encoded image. Here one key is needed to encrypt and decrypts the image, and then we had to applied compression techniques for a better compression and to prepare unrecognized and unreadable format. Finally, the Experiments are conducted to demonstrate the feasibility of the security is providing to the image in network security.

2. The Basic Principles

Encryption

Encryption is process the data or code has to convert into unreadable format. This processor helps in protecting the privacy while sending the data from source to destination. But at destination side the data decrypts and bought it back as it’s original. The process of reverse of an encryption is called decryption. This notion like encryption and decryption techniques needs some extra information for encrypting and decrypting the information. Such typed information is known as key. Here different types of keys are available to decrypts the encrypted data.

Authentication

Authentication is another important principle of cryptography. This is making sure that the idea was originated from the originator claimed in the communication. Presume, dispatcher dispatches information to receiver and now receiver wants evidence that idea has been certainly sent by dispatcher. This can be made possible if Alice performs some action on message that receiver knows only sender can do.

Integrity

The chief aim of this concept is in the cryptography is the excellence of being honest and having strong moral values. This means that Cryptography should ensure that the messages that are received by the receiver are not altered anywhere on the communication path. This can be achieved by using the concept of cryptographic hash.

Non Reputation

What happens if Alice sends a message to Bob but denies that she has actually sent the message? Cases like these may happen and cryptography should prevent the originator or sender to act this way. One popular way to achieve this is through the use of digital signatures.

2.1. Types of Cryptography

In the There are three types of cryptography techniques:

- Secret key Cryptography
- Public key cryptography
- Hash Functions
2.1.1. Secret Key Cryptography
One key is used in this technique. This one key is used by the applicant/sender to encrypt the image; later the receiver/applicant used this key to decrypt the image, i.e. in both sides the single key is used for the purpose of encrypts and decrypts the image. Hence the sender later encrypts the image by single key he send the key to receiver, then the receiver uses this key to decrypts the image.

But it’s a biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

2.1.2. Public Key Cryptography
Here, two keys are used in this type of cryptography techniques, one key is used in between sender and retriever involves providing to secure the information to send. Another one is used in between retriever and sender used to insecure the data. Since the pair of keys is applied here so this technique is also known as asymmetric encryption. In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob’s public key and Bob can decrypt the message with its private key.

2.1.3. Hash Functions
This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus. So we see that how different types of cryptography techniques (described above) are used to implement the basic principles that we discussed earlier. In the future article of this series, we’ll cover more advanced topics on Cryptography.

Input | Hash sum
--- | ---
Fox | DFCD3454
The red fox runs across the ice | 52ED879E
The red fox walks across the ice | 46042841
The Asymmetric method is also known as a public-key method. The key holder has two keys—a private key (which only they know) and a public key (which is uploaded to a key server or given to people they want to correspond with). When a person wants to encrypt a message or file, they use the Public key of the recipient to encrypt it. This ensures that only the recipient (or anyone with the private key) can read the message or file. If the sender wants to guarantee that they were the sender, they will use their private key to sign the message (and the recipient will use their public key to verify that it was sent by them). PGP and its open-source variation (Open GPG) are examples of asymmetric keys.

- **Final Thoughts**

One more important factor is key-length. While it is not a method, it still needs to be taken into consideration. The longer the key-length means the probability of a person cracking the key increases exponentially with the increase in bits. For example, a 2-bit encryption has four possibilities, so a 128-bit has 2128 possibilities. It is important to pick the strongest method and the largest key possible.

3. PROPOSED METHOD.

3.1. Forward Technique of proposed method

The following steps explained about the forward processor technique of the proposed work. As there is no header for raw images and easy to apply any techniques on this to get a better results. In this method, raw images considered as a source input image. Convert this source image into the digital format. Create a key using random generation technique. Apply the shift operation on digital format of source image along with this key. By this we get the encoded image. This format of image is called cipher image, this is hiding information in unreadable format. Simply encrypted format. To reduce the size encoded image compressed the image using Huffman compression technique. By this we get less size of image i.e. size reduced image and it is also helps to easily transfer even through the low bandwidth network also as easily and firstly.

- **Step1.** Consider raw image as an input file.
- **Step2.** Convert input raw image into digitized form.
- **Step3.** Generate Random Number
- **Step4.** Apply shift operation on input image along with random number to generate mask image.
- **Step5.** Apply compression technique on masked image to generate compressed image

3.2. Reverse Technique of proposed method.

The following steps explained about the reverse processor technique of the proposed work. In this reconstruct the image from above approach method we should take already encrypted and compressed image as a source image, uncompress the compressed image first, on this uncompressed image apply reverse shift operations, generate random number key and we get a digital formatted image and make it as original raw image. But here at the time reconstruction image if lose some information, that even eye may not considered, but we found it at comparison state of both images i.e. source image and reconstructed image.

- **Step1.** Take already encrypted and compressed image as an input file.
- **Step2.** Apply reverse Huffman compression technique on what you took an input file, then the resultant image shows as the mask image.
- **Step3.** Apply reverse shifted operation.
- **Step4.** Suppurate random key then form a digitized image.
- **Step5.** From digitized formation make source image.

![](pic_5.png)

4. Results

For this, an experimental analysis is one with the different raw images whose resolution is in different sizes. In this paper random number generation phases made the image in unrecognized format. The property of this entitled is to increase the security levels of the encrypted encoded image. Here one key is needed to encrypt and decrypts the image, and then we had to applied Huffman compression technique for a better compression and to prepare unrecognized and unreadable format. Finally the Experiments are conducted to demonstrate the feasibility of the security is providing to the image in network security. This method gives a better result than JPEG, BMP and TIFF, but few of image formats are better than of proposed method based on pixel intensity.

![](pic_4.png)

**Pic. 4** Foreword processor of proposed method

**Pic. 5** differences among different images in techniques
In this proposed the information is lossy, but the eye is can’t find the difference between original and retrieved. The followed tables and graphs gives analyzed and compared information about proposed content with existed techniques.

**Table 1: Comparison study of proposed method among different compression methods**

<table>
<thead>
<tr>
<th>Sn</th>
<th>Image Name</th>
<th>Raw Image Size</th>
<th>Raw Compression</th>
<th>JPEG</th>
<th>TIFF</th>
<th>Proposed Compression</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Baboon</td>
<td>13634</td>
<td>15119</td>
<td>28775</td>
<td>27276</td>
<td>14730</td>
</tr>
<tr>
<td>2</td>
<td>Brain</td>
<td>12010</td>
<td>8807</td>
<td>17776</td>
<td>22016</td>
<td>9197</td>
</tr>
<tr>
<td>3</td>
<td>Lena</td>
<td>21025</td>
<td>19659</td>
<td>24650</td>
<td>31248</td>
<td>19060</td>
</tr>
<tr>
<td>4</td>
<td>Madhuri</td>
<td>16368</td>
<td>15232</td>
<td>22340</td>
<td>25776</td>
<td>14593</td>
</tr>
<tr>
<td>5</td>
<td>Pepper</td>
<td>16368</td>
<td>15204</td>
<td>22285</td>
<td>25848</td>
<td>14804</td>
</tr>
<tr>
<td>6</td>
<td>Head Scan</td>
<td>15625</td>
<td>14216</td>
<td>19431</td>
<td>24940</td>
<td>13967</td>
</tr>
<tr>
<td>7</td>
<td>Shoulder</td>
<td>18225</td>
<td>14110</td>
<td>21612</td>
<td>28244</td>
<td>13925</td>
</tr>
</tbody>
</table>

**Graph 1:** Show Comparison study of proposed method among different compression methods.

To calculate the compression ratio by the equation, and proposed technique is compare with different compression technique, which is given better results than of existed techniques.

**Table 3: Comparison study of proposed saving percentage among different images formats saving percentage**

<table>
<thead>
<tr>
<th>Sn</th>
<th>Image Name</th>
<th>JPEG CR</th>
<th>TIFF CR</th>
<th>Propose compression Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Baboon</td>
<td>0.56933</td>
<td>0.60675</td>
<td>1.112288</td>
</tr>
<tr>
<td>2</td>
<td>Brain</td>
<td>0.70938</td>
<td>0.57265</td>
<td>1.261099</td>
</tr>
<tr>
<td>3</td>
<td>Lena</td>
<td>0.85398</td>
<td>0.67284</td>
<td>1.263095</td>
</tr>
<tr>
<td>4</td>
<td>Madhuri</td>
<td>0.73339</td>
<td>0.65563</td>
<td>1.12273</td>
</tr>
<tr>
<td>5</td>
<td>Pepper</td>
<td>0.73520</td>
<td>0.63859</td>
<td>1.167672</td>
</tr>
<tr>
<td>6</td>
<td>Head Scan</td>
<td>0.80412</td>
<td>0.62650</td>
<td>1.313265</td>
</tr>
<tr>
<td>7</td>
<td>Shoulder</td>
<td>0.85351</td>
<td>0.64527</td>
<td>1.308797</td>
</tr>
</tbody>
</table>

**Graph 3:** Comparison study of proposed saving percentage among different images formats saving percentage.

When we observed the above the data the proposed technique is given better results than existed compression techniques.
5. Conclusion

In this paper, we propose a lossy compression scheme for pixel-value encrypted images. The main contribution of our work is shown as:

- The experimental results show in sizes and compression rates that our proposed scheme achieves much better performance than the existing lossy compression scheme for pixel-value encrypted images, and also achieves similar performance as the state-of-the-art lossy compression on the pixel permutation-based encrypted images.

References


Author contributions

Mr. G. Thippanna, Research Scholar (Ph.D.). He has completed his Post Graduation in 2008 from S.V. University, Tirupati. He has 4 years of teaching experience and 4 years of research experience, till now 4 international papers.

Dr. T. Bhsakara Reddy, Associate Professor. Department of Computer Science and Technology at S.K University, Anantapur A.P. He holds the post of Deputy Director of Distance education at S.K. University and he also the CSE Coordinator of Engineering at S.K. University. He has completed his M. Sc and Ph. D in computing science from S.K. University. He has acquired M. Tech from Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 17 years. He has published 47 National and International publications. He has completed major research project (UGC), Four Ph. D and three M. Phil have been awarded under his guidance. His research interests are in the field of image Processing, computer networks, data mining and data ware house.

Dr.S.Kiran is an Assistant Professor in the department of Computer Science and Technology at Yoganvena University, Kadapa, A.P. He has completed his M.Sc and Ph.D in computing science from S.K. University. He has acquired M. Tech from Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 5 years. He has published 4 National and International publications. His research interests are in the field of image Processing, computer networks, data mining and data ware house.