IMAGE PRIVACY PROTECTION AS A SINGLE SHARE

Shincy Richu Jacob[1], Hari S.[2], Anju K. Abraham[3]

[1]PG Scholar, Electronics and Communication, Mount Zion College of Engineering, Kerala, India
[2,3]Assistant Professor, Electronics and Communication, Mount Zion College of Engineering, Kerala, India
---***---

Abstract - *Visual data has become a necessary element in the day-today life. With the increased usage of visual data, the threat to the data also increases proportionally. Therefore, a system is required to protect the visual data. In this paper, a method has been proposed to provide privacy protection using false color, within JPEG architecture. This becomes more beneficial in a sense that it adds on an advantage of reducing the file size, decreasing the complexity. For creating the protected file, JPEG encoding-decoding, AES encryption and zlib compression is used, which finally results in protected image as false image with metadata. For recovering the original image, the inverse process is adopted, where the protected image is decompressed, decrypted and then decoded, resulting in recovered image. Since zlib compression is a loseless compression method, the recovered image will be exactly as original image. This scheme provides a high level of privacy conservation since the original data can only be recovered by authorized person and not by any illegitimate user upto a great extent. On a higher practical level the scheme can be used for surveillance system, thus also providing intelligibility and privacy. The results show how the false image can be used for the privacy protection of visual data.*

Key Words: AES, Color palette, False image, JPEG, Metadata, Privacy protection, Visual data, Visual cryptography, zlib

1. INTRODUCTION

The first ever picture that was ever taken was the View from the window at Le Gras by Joseph Nicephor Niepce in 1826. Then came the first ever picture containing a person, which was taken by Louis Daguerre in 1838. Since then a lot of changes occurred. The evolution from pinhole camera to DSLRs has led to a lot of images being taken. Not only the images are produced but also they are being shared at a humongous amount over internet. It is said that Snapchat users share 8796 photos a second. According to Internet.org whitepaper, in 2013, every day over 350 million images were shared on Facebook. Thus, we can say that the modern age embarks the usage and transmission of more and more multimedia data. It has become a cliché in this era of transferring the visual data. Then arises a question for the protection of privacy of the images that we transmit and receive.

It is recorded in Mary Meeker's annual Internet Trends report of 2014 that civilians uploaded upto 1.8 billion digital images every single day. That's 657 billion photos per year i.e. for every 120 seconds people take more photos that ever existed. Thus, we can say that the popularity of social media for posting pictures has given rise to a new type of mediated communication called online photo sharing. [1]

More interesting fact is that these 657 billion numbers of images are the ones that are uploaded online, that means this doesn't include images stored on our computers. That would increase the number beyond imaginable level. It also doesn't include security camera footages i.e. other than the images we take ourselves and share, there comes the question of privacy concerns for an individual by the surveillance systems as well.

In India, video surveillance technology has been establishing to a large level. The usage of CCTV surveillance systems is increasing everyday mainly due to increasing fear of terrorism and the availability of cheaper cameras. According to Times of India news report of 2016, Delhi itself has installed about 1,79,000 CCTV cameras. [2]

It has been said that the United Kingdom has around 6 million surveillance cameras. According to CrimeFeed, an average American is captured on camera 75 time a day. According to industry estimates, it has been stated by Economic Times that over 2 million surveillance units is being sold every month. Thus, we can imagine the number of eyes on us while we just wander around. This will leave us in a havoc of our privacy like that of our identity, location etc. so it will be reasonable to provide privacy protection methods, as such that the data could only be accessed by authorized person.

There exist a bunch of privacy protection methods. The problem with those are they conventionally require either manual or a computer module for identification of sensitive regions, hence giving rise to complexity that in turn affects reliability. There exists some cloud security solutions but those are also improper as they tend to out-turn the original image into a scrambled image that would be unrelated to the original image.

This paper brings forth a method that could be reliable for the visual data privacy protection and provide intelligibility and robustness with security. We rely on the concept of false color within the JPEG architecture. It includes color palettes, which is a major concern to generate the false image. To ensure that the false image is secure from illegitimate users, compression and encryption is additionally provided. Further, we will show the result of the scheme based on different color palettes.

2. Related Works

When we take visual data into consideration, our motto is to provide its security in a manner that its sensitive information is not revealed to any person who views it but only be visibly understandable by person who is authorized to get the data.

In 2011, Constantinpopescu et al. [4] proposed a method for secure e-cash transfer which was based on the elliptic curve discrete logarithm problem. In this method, the elliptic curve discrete logarithm method was used to send a secure encrypted message using public key and at the receiver side the encrypted message was retained by the respective private key.

Similarly, a visual cryptographic biometric template [5] was proposed, which worked by means of the random permutation. This technique had shown that it has enhanced the safety of visual cryptography by scrambling the image by means of random permutation.

There was a method proposed for crypto system based authentication using CSTA (Cyclic Shift Transposition Algorithm) [6]. In this method, the CSTA was used to send the encrypted message as symbols and only the receiver receives the encrypted message which was decrypted by their private key for retaining the original message.

A technique was proposed in 2013, [7] which was for the visual cryptography using compressed random shares. In this technique, the visual cryptography scheme consisted of n number of transparent shares with condensed dimension and supported a diversity of image designs in addition to offering an integrated approach for binary, gray and color image visual cryptography by preserving the visual excellence and pixel growth.

Hao-KuanTso *et al.* [10] proposed the innovative technique for medical image sharing by using the random grids. In this technique, the random grids were employed to build two insignificant shares. Thereafter, a friendly model was overlaid on the shares in such a manner that the users were capable of dealing with them and recognizing them effortlessly.

Another method involving a visual data protection strategy was proposed by K. Shankar et al, [12] in which the images would be transmitted as shares. The proposed system was a visual cryptography method which is used to send the image to the receiver in a secure manner, protecting the information of the image. The image is transmitted to receiver as shares and all shares are stacked together by the receiver to get back the original image. The pixel values of the image are firstly extracted from the original image. Now, these pixels values are used to create the multiple shares. Then the shares are encrypted by using the elliptical curve cryptography (ECC) and transmitted. At the receiver side, the shares are decrypted using ECC decryption method and then all the decrypted shares are stacked over each other to get the original image. This paper provides security without any distortion to the image but the issue which comes with it is that a number of shares (4 shares for each of the 3 colors i.e. 12 shares) has to be created, thus consuming the storage space. Further, the complexity is high since each of the shares has to be encrypted individually.

Recently, false colors have been used for the purpose of visual privacy protection. In that respect, a RGB input image is first converted into grayscale. The grayscale value is then used to index into RGB color palette and the corresponding RGB triplet is used to replace the original pixel value of the image.

The primary advantage of false color based privacy protection is that it can be applied on the entire image without compromising with the intelligibility of the image as well as the original content can be exactly recovered. A single JPEG image output is developed in which the main image is the protected with some additional information saved in the metadata of the JPEG image. An authorized person can only decrypt the extra information to recover the original.
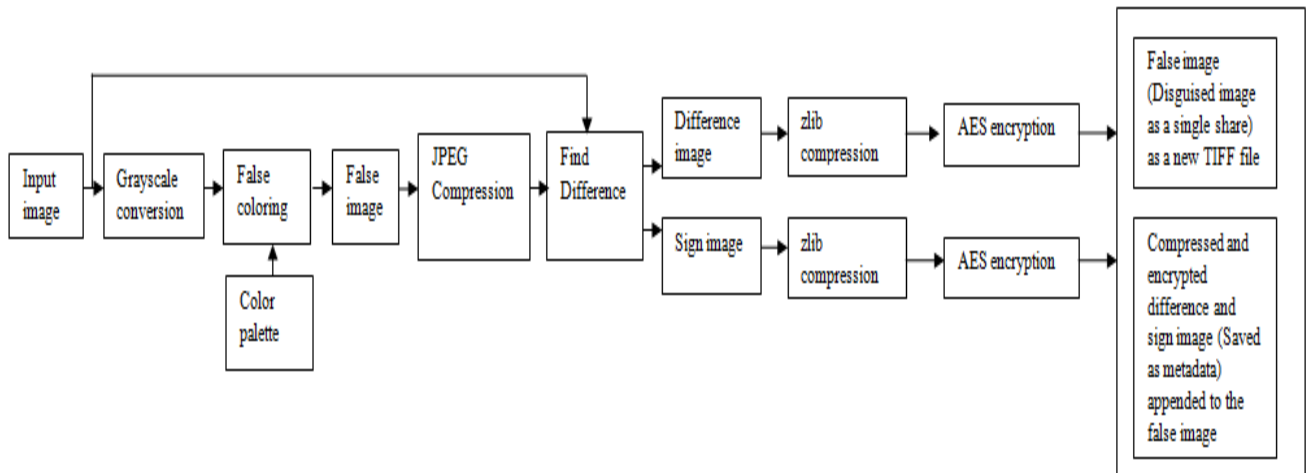
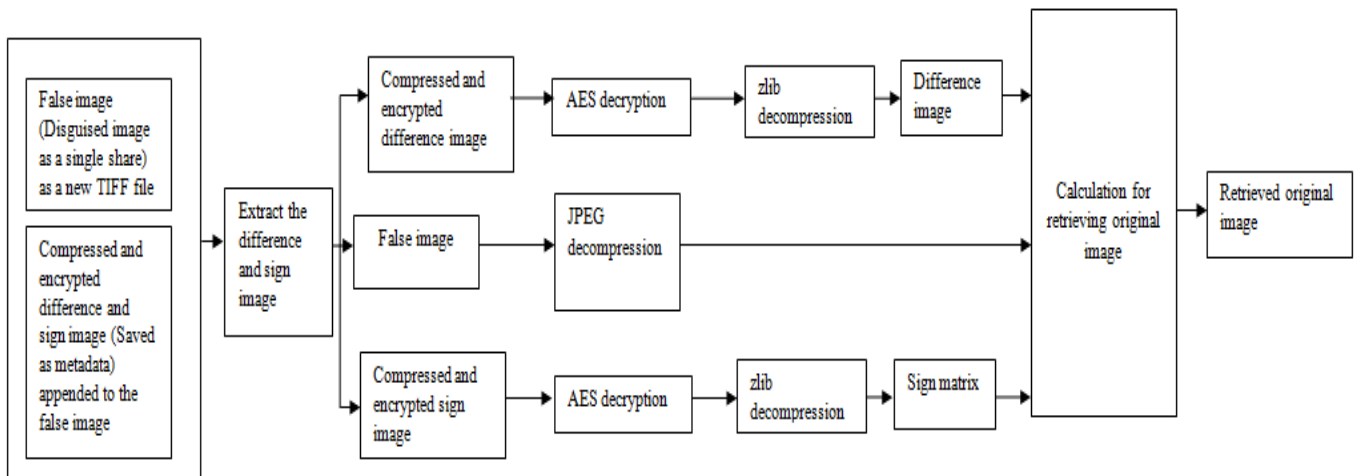Fig. 1 Block diagram of the safeguarding algorithm

Fig. 2 Block diagram of the retrieving algorithm

3. Proposed System

The proposed method consists of the scheme in which false coloring is used, it can be used with any privacy protection strategy. Firstly, the steps for safeguarding the image is briefly given and then the steps for retrieving the original image is given.

1) The safeguarding algorithm

The scheme begins with the input image (I) being converted into grayscale image, Ig. Next, by using the grayscale values as indices into a color palette, the false color image (FI) is obtained. The false image then undergoes JPEG encoding and decoding.

Thus, resulting in FI'. Then the difference image (DI) is computed by subtracting JPEG encoded false image from input image, i.e.

$$DI = I - FI'.$$

This difference can somewhat be negative, hence a sign image is computed as,

SI = 1, if I – FI' < 0 or

SI = 0, elsewhere.

The difference image and sign image is then compressed either losslessly or lossily. If lossless compression is considered, zlib compression is implemented otherwise JPEG compression is used, if lossy compression is considered. In this paper, we use zlib compression algorithm.

The compressed difference image and sign image is then encrypted using AES (Advanced Encryption Standard) technique, which is done by providing a hexadecimal key.

The false image is then written into a new TIFF file and the compressed and encrypted difference image and sign image are appended into the image i.e. saved in the form of metadata. The final output thus being the protected image i.e. the false image with the difference and sign image stored as metadata.

2) The retrieving algorithm

For getting the original file, the JPEG files that are to be recovered will be the false image of the original image that will be carrying the difference and sign image.

Hence, we can state that the image can only be recovered if the metadata is provided with it, which is possible to be recovered by an authorized person. The protected image will be decoded to obtain the false color image, difference and sign image accordingly.

The retrieved image R obtained from this technique will be similar to the original image I, to a large extent because here the difference image (DI) is losslessly compressed. Thus, the method is somewhat superior to other methods where the recovered image deviates from the original image.

The JPEG file is first decrypted by AES technique using the authorization key that was used at the time of encryption. Then, the decrypted image is decompressed by zlib decompression method.

Then the false image is JPEG decoded that will be FI'. Finally, the original image will be obtained as recovered image, R, which is obtained as,

$$R = FI' + s\,DI$$

where,   s = 1, if SI = 0 or

s = 0, elsewhere.

4. Result

In order to show the validity of the proposed method, the algorithm is implemented in MATLAB and the corresponding result is demonstrated for a normal image (in case of securely transmitting and receiving an image, without the data being revealed to an attacker) and an image with a human face (in case of prevention of privacy for surveillance system) and that would be shown using four different color palettes.

It is pretty clear from the result that the complexity of multiple shares has been solved as a single image does the work of protecting the original image in a form that the image becomes unrecognizable and not so easy to crack.

In Fig. 3, the first image to be taken is that of a human face which is converted into false image by using two color palettes known as 16_Level and accent. In both the results (a) band (b), the output image is seen to be completely like a camouflage i.e. as a disguised image, anyone having a look at the image would instantly know that it's the face of a human and we can spot the features of the face but the irony is that it isn't possible to know who that particular person as it is seen as a

false image. So, it is precisely effective in preventing the privacy of a person whether their image is captured by surveillance system or the picture has been used for transmission.

The other image taken is that of an infrastructure which is just to give reference to an image which could be other than a human face, which we use for transmission that should not reveal the information of the image to any unauthorized person who tends to view the image being transmitted or received. There are two color palettes used for creating the false image, namely flag and waves. In the output (c), it can be seen that the disguised image is completely unrecognizable to any person who views it. Comparatively, the output in (d) also makes the image unrecognizable but if we want the image that is being sent to not just be unrecognizable by a third person but also to be more defensive, it is better to use the flag color palette.
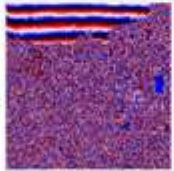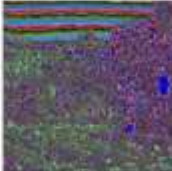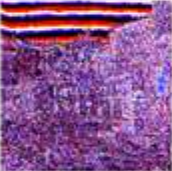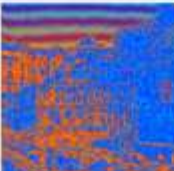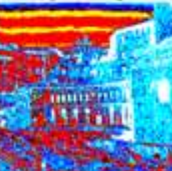
Fig. 3 Result of the code implemented shown on 2 images with their respective disguised image, difference image and sign image, using four color palettes: (a) 16_Level (b) accent (c) flag (d) waves

For both the original images demonstrated, it is visible that we require just a single share of image to be encrypted and transmitted, rather than multiple shares. Hence, making the system much less complex and saving the storage space. Other than that, the method provides an ample amount of protection to our images that we are meant to use on a daily basis for sending as well as in surveillance system, providing the relief of being in safe hands.

5. Conclusion

The paper has put forward a privacy protection method for visual data, which was implemented within the JPEG architecture. After the implementation of the respective code in MATLAB, the result has been demonstrated. As a result, it can be said that the method is very much effective if we consider human observers of the image for whom it would be visually a tight spot to identify the image.

The selection of a suitable color palette is a very important consideration for this method. These palettes are bound to provide high security to our image but it would be more relevant if we define the color palettes particularly meant for privacy protection purposes. But still considering all the advantages, the dependence of result on the color palette is not that much a weakening factor. In fact that is just to let know of the fact that which color palette will be suitable for which application. Similarly, an important consideration is that of the key used for AES encryption. Since it is symmetric encryption, we need to consider securely transmitting the key. Further, for future work, asymmetric cryptography in case of keeping the key secure can be considered but keeping in mind that it could increase the performance time.

The concept of storing the difference and sign images as metadata helps in a greater reduction in file size compared to the other methods. Being a metadata, the difference and sign images are part of the image itself but certainly only known to the authorized person, who is the only one knowing the key by which the person can recover the respective difference and sign images and then only in turn recover the original image.

REFERENCES

[1] Anne Oeldorf-Hirsch and S. Shyam Sundar "Social and Technological Motivations for Online Photo Sharing" Journal of Broadcasting & Electronic Media, 60:4, pp. 624-642, 2016.

[2] Sanchita Hasija and Shruti Nagpal, "CCTV Surveillance in Public Spaces of Delhi: Exploring the Perspectives of Youth visiting Malls and Delhi Metro," IOSR Journal Of Humanities And Social Science Volume 23, Issue 12, Ver. 2, pp. 4-8, 2018.

[3] S. B. Sadimon, M. S. Sunar, D. Mohamad, and H. Haron, "Computer generated caricature: A survey," in Cyberworlds (CW), 2010 Intl. Conf. on. IEEE, pp. 383–390, 2010.

[4] Constantin POPESCU, "A Secure E-Cash Transfer System based on the Elliptic Curve Discrete Logarithm Problem", Journal of Informatica, Vol.22, No.3, pp.395–409, 2011.

[5] Rahna P. Muhammed, "A Secured Approach to Visual Cryptographic Biometric Template", Journal of Network Security, Vol.02, No.3, pp.15-17, 2011.

[6] R.Kalai Selvi and V. Kavitha, "Crypto System based Authentication using CSTA in Grid" International Journal of Computer Applications, Vol.48, No.22, June 2012.

[7] L. N. Pandey and Neerajshukla, "Visual Cryptography Schemes using Compressed Random Shares", Journal of Advance Research in Computer Science and Management Studies,Vol.1,- No.4,pp.62-66,2013.

[8] P. Korshunov and T. Ebrahimi, "Using face morphing to protect privacy," in Advanced Video and Signal Based Surveillance (AVSS), 2013 10th IEEE Intl. Conf. on. IEEE, pp. 208–213, 2013.

[9] P. Korshunov and T. Ebrahimi, "Using warping for privacy protection in video surveillance," in Digital Signal Processing (DSP), 2013 18th Intl. Conf. on. IEEE, pp. 1–6, 2013.

[10] Hao-Kuan Tso, Tsung-Ming Lo, and Wei- Kuei Chen, "Friendly Medical Image Sharing Scheme", Journal of Information Hiding and Multimedia Signal Processing, Vol.5, No.3, pp. 367-378, 2014.

[11] J. R. Padilla-L´opez, A. A. Chaaraoui, and F. Fl´orez-Revuelta, "Visual privacy by context: a level-based visualisation scheme," in Intl. Conf. on Ubiquitous Computing and Ambient Intelligence. Springer, pp. 333–336, 2014.

[12] K. Shankar and P. Eswaran, "RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography", China Communications, pp. 118-130, 2017.