A Secured and Accessibility Controlled Sharing of Images with Multiple Users

S. Lakshmi Narayanan[1], K. Sankaranarayanan[2], V. Vijayakumari[3]

[1] Electronics and Communication Engineering, Sri Ramakrishna Engineering College, India
[2] Electronics and Communication Engineering, P.A. College of Engineering and Technology, India
[3] Electronics and Communications Engineering, Er. Perumal Manimekalai College of Engineering, India
shrinarayanan20@gmail.com, kkdcbesankar@gmail.com, ebinviji@rediffmail.com

Abstract

The creation of Multimedia images and files has been increasing day by day that in turn leads to suspicious acts and threats. Many research works have been preceded for the same. In the recent works, confidential image data security based on encryption and watermark (CIDSEW) was proposed in which security features. Here, secrecy information is incorporated with the images, to be shared through watermarking technique. Nevertheless, it doesn't give a secure way for access restriction when it goes for multiple users because the encryption algorithm used implants the whole image which weakens the functioning where the sensitive parts of the images can't be centered approximately. The major aim of the proposed work is to introduce a new security algorithm for secure sharing of text via the watermark image. In order to overcome the restrictions in the existing technique, the novel approach namely Secured and Attribute based User access control (SA-UAC) methodology has been presented in the proposed work. The proposed work is done in MATLAB which demonstrates that the proposed work prompts the preferred result. The results of the proposed and existing methods are measured in terms of Peak Signal-To-Noise Ratio (PSNR), Mean Square Error (MSE) and Correlation.

Keywords: Access control, Embedding, Water marking, Sensitivity, Encryption

1 Introduction

Image sharing is a service used to publish the photos on the web by which you can upload, manage and share your photos in public or secretly [1].

It is facilitated by both websites and applications which consist of photo galleries that are available online, wherein particular users establish and handle them, comprising blogs concerning only photos.

Other users can see yet not really download pictures, and they copyright options for their pictures at the time of sharing can choose unique Photo blogs allow displaying only a sequential view of photos which are user-selected medium-sized. But nearly all of the sites which are based on photo sharing present several outlooks and grant access for categorizing photos into albums, as well as insertion of annotations. The applications pertaining to desktop photo management might take account of having their own photo-sharing features or it may be incorporated with other sites for uploading the images and sometimes it's one and the only function is to share images, normally using peer-to-peer networking. Some applications allow you to do basic image sharing functionalities like email photos, which can be dragged and dropped into patterns that have been pre-designed. Sharing of images isn't limited only for the web as well as the PCs, except to a certain extent it can be similarly imaginable from gadgets which are convenient, for example, camera telephones, either specifically or by means of Multimedia Messaging Service (MMS) [2].

As the technique of Image sharing has turned out to be a high-flying sector in both large as well as small networks, Security is an important aspect to be taken into account. For the shares to be distributed to their respective shareholders, a secure channel's required for the purpose of protecting the shares from possible assaults on the network by various other users. If such other consumers are capable of locating the minimum required number of shares then the image can be recovered by them by utilizing the Lagrange interpolation method. To sort out these issues Secret image sharing (SIS) [3-4] is being used broadly used in the last ten years in which the secret image is segregated into various random image shares (say k) [5-6], that have been distributed to various consumers and only smallest amount of shares (say $t \leq k$) is required for the retrieval of the secret image.

Here, a quite challenge is their safe delivery over an unsafe network, even though image shares are random plus there is no information being exposed concerning the individual shares pertaining to the secret image. In order to protect the images from an opponent, we need to take on a solution which is (t, k)-SSS based; through

*Corresponding Author: S. Lakshmi Narayanan; E-mail: shrinarayanan20@gmail.com
DOI: 10.3966/160792642020032102015

this we can send at the camera shares of captured image by the base station via various courses.

Nevertheless, an opponent close to the base station has the ability to capture t or additional shares easily furthermore recreate the secret image; this solution does not assure security. So we are in need to adopt a tough encryption algorithm like Advanced Encryption Standard (AES), to encrypt the share images. However this is very costly, particularly in a scenario of a wireless network in which the camera nodes' computation power is not enough.

To overcome all these issues, the proposed research work uses secured and access controlled image sharing technique that focuses privacy.

Secured and Attribute based User access control (SA-UAC), is used in the proposed work which controls the user access while sharing the secret images. This, in turn, provides the preferred result on user access permission restriction than the current work. To provide this result, the set of users who endeavor to use the same images are shared via single medium by restricting their access permission. Next, is the security features for the images, which is accomplished through segmentation, only the sensitive part of the images will be watermarked and encrypted, instead of whole images.

2 Related Works

This section deals with various related research works on the subject of secured secret image sharing is discussed. In dithering technique uses (k, n) threshold visual cryptography scheme pertaining to images that are gray level, in which the decrypted image's reduction size is obtained although the decrypted image's quality depends on the quality of the halftone image [7]. By employing Adaptive order technique, of the gray-level image, the half-toning is performed by utilizing a curve meant for space-filling for achieving deviation that is adaptive of the size of the cluster.

In the technique of half-toning, the encryption [8] is performed by changing the gray level image into the fairly accurate binary image or else a half tone image possessing 0 and 1 as pixel values. For example, considering case of (2, 2) - VCS, the secret image is segregated into two shares by the step. In the process of decryption, by using mound binary shares, recreation of the original image is done. In Sandeep Katta [9] Two-out-of-Three Scheme, he combines any of the two shares that'll show the real bit information, (although not the entire share) only a part of every individual share will provide a image of high-quality while it is recreated.

Naor and Shamir [9] introduced a visual cryptography to achieve secrete sharing, it encrypts information which is visual in a manner such that the decryption is performed by means of the human visual system known as Visual Cryptography Scheme (VCS). According to this technique, a combination of black and white pixels for a secret image would be taken and for generating the share each pixel is operated separately. Encoding scheme divides the binary image into two shares. Likewise, in case there is a black pixel at that time anyone of the two rows beneath is preferred for the purpose ofproducingshare1 and share2.But in this method, it does not provide any hint whether the pixel is found to be black or white. The generation of the Secret image occurs only at the time when both the shares are overlaid.

Superimposing of the embedding images can be done to decode hidden messages. Liguo Fang [10] suggests a scheme which is (2, n) on the basis of permutation to balance the performance amidst pixel expansion and contrast. Xiao-Qing and Tan [11] recommend schemes like Threshold visual secret sharing which unite operations like XOR with OR by reversing as well as based on binary linear error correcting code. For encoding the secret, it divides the image which is original into n number of modified versions in order that every pixel present in a share is subdivided into m number of black as well as white sub-pixels. For image decoding, select a subset S concerning that n number of shares and each of them is copied on top of a precision. Supposing S represents a "qualified" subset, in that case mounting all of the transparencies shall permit visual recovery of the secret image.

Crampton and Pinto [12] start by examining the representation of access control policies and measure alternative secret-sharing schemes with the purpose of could be used to enforce them. Kaaniche and Laurent [13] proposed a multi-level access control mechanism depending on an original use of attribute based encryption schemes. Initially, it ensures fine-grained access control, behind multi-security levels with value toward diverse granted access rights designed for every outsourced data file. Second, depending on an attribute based algorithm, key management is minimized; such with the purpose of users sharing the same access rights are not needed in the direction of collaborate to extract the secret enciphering key. Third, proposal is proven in the direction of give capable processing and communication overhead, compared toward traditional procedure of attribute based encryption schemes.

3 Secured and User Access Control Aware Secret Image Sharing

Secured and Attribute based User access control (SA-UAC), is used in the proposed work which controls the user access while sharing the secret images. This, in turn, provides the preferred result on user access permission restriction than the current work. To provide this result, the set of users who endeavor to use the same images are shared via single medium by

restricting their access permission. Next, is the security features for the images, which is accomplished through segmentation, only the sensitive part of the images will be watermarked and encrypted, instead of whole images. The proposed work is accomplished by through the following ways:

- Segmenting the sensitive part of image from the entire image
- Watermark the secret information
- Integrate the access permission details with the watermarked image
- Encrypt the image using attribute-based encryption

Through the unsecured medium, along with user access restriction, security and secret image sharing is achieved. In the upcoming sections, the proposed work is explained in detail. The overall representation of the proposed work is shown in Figure 1.

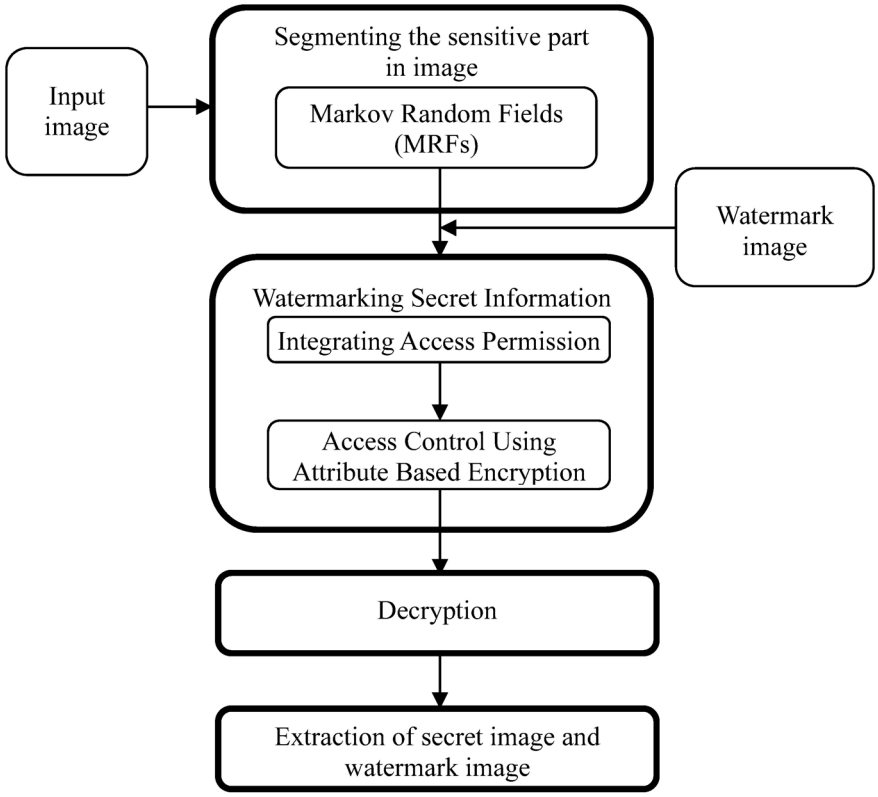

Figure 1. Overall architecture Secured and Attribute based User Access Control (SA-UAC) system

3.1 Segmentation of Sensitive Parts of Image

A normal image not only contains the required contents, it includes some noises also. They may also contain some unwanted background contents too. While handling these unwanted contents in the images, may prompts to some serious issue like memory issues during storage, bandwidth problem while sharing and it goes on. To overcome these issues, only the sensitive part of the images should be gathered from the whole image, which is obtained through segmentation process. It segregates the foreground image from the background images.

The Proposed work presents, learning based classification segmentation to handle the segmentation process. In segmentation of an image, classification which is learning –based pixel and region is considered as one of the famous approaches.

3.1.1 Markov Random Fields (MRFs)

Markov Random Fields (MRFs) [14] is taken as representative case of learning-based region classification. As indicated by MRFs, either at the level of the pixel or at the level of patches concerning predetermined spatial scale (size), the images are partitioned into various sites. Every site represents: (i) a hidden node or label node, this is a hoped node to calculate the particular site: in region segmentation, this node is considered as a region of interest or background, (ii) observation or feature node, represents to feature set of the site, which is predicted in a straightforward manner from the images. So the segmentation result has become the optimization problem globally, that is, predicting the label field which is desired from the observation. On the other hand, conventional deformable models proceed with deterministic energy minimization approach which doesn't give predominate result so in proposed work learning-based classification methods are utilized on the probabilistic solution, that is the maximization of probability.

3.2 Watermarking Secret Information

To provide protection and security to the images, the secret information would be embedded with the images, after segmenting the region of interest part from it. In order to safeguard the corruption of embedded secret data, secret key authentication based watermarking is introduced here. Let us take an image which is of gray scale $x_{m,n}$ having a size MX by NX in pixels. In order for the formation of a watermarked image having the same size, an invisible watermark has to be inserted.

For achieving it, $x_{m,n}$ is first partitioned into blocks of pixels of I×J. Subsequently insertion of an invisible watermark into every block of image data is done. Consider am, to be an image which is bi-level that might be used like a watermark which is invisible that needs to be embedded in $x_{m,n}$. Here, am, n need not necessarily be in a size equal to $x_{m,n}$. Another bi-level image $b_{m,n}$ having a size MX×NX (similar size as $x_{m,n}$) from $a_{m,n}$, is created.

Even though there are many ways to do so, bm, n by the process of tiling am,n, that is, replicating am, occasionally to the size which is required is created. Other option, given the size difference between $x_{m,n}$ and $a_{m,n}$ is little, it is to add all of the zeros (or all of the ones) to the $a_{m,n}$ boundary, in such a way that $b_{m,n}$ of the desired size we can acquired. Consider,

$$X_r = \{x_{iI+k,jI+1} : 0 \le k \le I-1; 0 \le 1 \le J-1\}$$

Has been used as a block of size as I×J acquired from the image $x_{m,n}$. In order to make it simple, a single index r to indicate the r^{th} block in the image is used. The block which is equivalent contained by the binary image $b_{m,n}$ is represented using

$$B_r = \{b_{iI+k,jI+1} : 0 \le k \le I-1; 0 \le 1 \le J-1\}$$

Let, a cryptographic hash function be given by

$$H(S) = (d1, d2, \ldots, dp)$$

Here, S stands for a data string with an arbitrary length, di's will be the bits of the binary output concerning the hash function, and p represents the output bit string's size. H refers to cryptographic hash function which produces an output (d1, …., dp) by giving S as an input. But, this is unfeasible computationally for finding out another bit string concerning the input of every length that might be hashed to the similar output (d1, …., dp).

A well-known example is MD58. In this algorithm, the data string is hashed into a bit array having a length 128, that is, p = 128.

Consider K to represent user key which contains bits as a string. Also create the equivalent block X_r designed for every datablockX_r, where every element present in $\tilde{X}_r$ will beidentical to the consequent element present in X_r apart from that the slightest significant bit is fixed at zero. For each block, the hash is calculated

$$H(K, Mx, Nx, \tilde{X}_r) = (d_1^r, d_2^r, ..., d_p^r)$$

In this instance, if p< I×J, expansion of the p bits which comprise the hash output by replication is done and dm, n, a rectangular array is constructed having the size I×J. Supposing not* if p>= I×J the primary bits I×J to produce $d_{m,n}$ is considered. To produce a novel binary block Cr utilizing a pixel by pixel exclusive OR operation, we combine the array $d_{m,n}$ with Br. This is how, we produce

$$c_{m,n} = b_{m,n} \oplus d_i$$

Here, $c_{m,n}$ refers to the elements present in Cr and $\oplus$ is exclusive OR operation. As a final point, To produce the output watermarked image block X_r^w, we place cm, n into the bit of the block $\tilde{X}_r$ which is considered as least significant. This course of action for each block of details repeated, and each and every one of the output blocks X_r^w isunited to produce the watermarked image $X_{m,n}^w$. To form a block $\tilde{Y}_r$, the bits of every element present in the block Y_r which is least significant is getting on with it to zero. To produce a block pertaining to the watermark of the output binary, we calculate H (K, MY, NY, $\tilde{Y}_r$) for every data block Yr and a pixel by pixel exclusive OR operation with Gr is performed.

This technique permits finding of any alteration made to an image which is watermarked as well as the verification of ownership by means of a secret key K. It is further used for watermark embedding and identified merely to the owner.

3.3 Integrating Access Permission Details

While using the secret (confidential) images, access permissions of the selected images should be checked, like viewing, editing, printing, backup, import and export features. In addition, the feature ought to manage the rights like open times, print amounts, usage lifecycle as well as time span. Moreover, for encryption as well as key management, the result will be able to impose user access management policies which are very granular, least-privileged, which ensures to protect data from the illegal access by means of users who are privileged along with APT attacks. Granular privileged user access management policies are enforced to various parameters like user, process, file type, time of day along with few others. Options pertaining to enforcement are utilized not just for permission concerning access to the data but also for what type of commands for a file should be avail for what kind of available users. Following access permissions are considered in the proposed work:

- View permission
- Edit permission
- Print permission
- Save permission

To elicit the security in the system, the mentioned permissions are applicable only for the users, to whom the confidential images are shared with.

3.4 Improved Security and Access Control Using Attribute Based Encryption

Attribute-based access control (ABAC) denotes a prototype that provides admission rights for the users by policies, which in turn blends the attributes [15]. The policies utilized in this work can employ any kind of characteristics like user attributes, resource attributes, object, environment attributes etc. Here in this particular representation, we use Boolean logic, that follows "IF, THEN" statement, like who is the person initiating the request, the resource along with the corresponding action to be taken place. For instance: IF the requesting person is considered as a manager, THEN permit access to read/write a sensitive data.

Role-Based access control (RBAC), as like the name it symbolizes the pre-defined roles which allow the certain set of access permissions that are associated with them to the users. The main difference with Attribute-based access control (ABAC) is, it follows Boolean rule set that can blend various attributes. [16] The values of the attribute can be set-valued or atomic-valued. Attributes concerning set-valued have above one atomic value like role as well as project, whereas attributes which are atomic-valued have just one atomic value. Like clearance along with sensitivity. It enables relation-based access control, where attributes are related to static values otherwise related to each other.

Access controls ideas that are Role based and relation based last for many years, to give a change for these ideas, ABAC is dealt the "Next generation" model for authorization.

Since this gives a dynamic, content-aware as well as risk-intelligent access control in order to assert which permits the access permissions policies that incorporate particular attributes from a wide range of data frameworks to be characterized to determine an approval and accomplish an effective administrative stability, permitting endeavors adaptability in their usage in view of their current foundations. In order to give a better security, Cipher text based attribute encryption is utilized in proposed work.

The private-key of the user is related to the attributes set in cipher text-policy attribute-based encryption (CP-ABE), in the framework cipher text provides access policy on the defined universe of attributes. Decryption of the cipher text can be done as long as the features satisfy policies concerning the corresponding cipher text.

The attributes determine the policies using conjunctions, disjunctions as well as(k, n)-threshold gates, that isk out of n attributes should be given (likewise, non-monotone get to strategies with extra negations and in the meantime there are additional developments for policies characterized as arbitrary circuits). For example, consider the universe of attributes as {A, B, C, D}, the key is got by user 1 for the attributes {A, B} furthermore user 2 gets the attributes fir {D}. When a cipher text is encrypted as concerned to the policy $(A \wedge C) \vee D$, so user 2 can decrypt but the user 1 cannot.

Thus, CP-ABE permits authorization implicitly, that's the user authorization is incorporated within the encrypted data. Another good thing is, the private keys can be received by the user if and only if the encryption of the data has been performed considering the policies. Encryption could be done with no knowledge of the users; we can do data decryption only by determining the corresponding policy. In future, if any other user receives the key as regards to the attribute and satisfying the policy can decry the text.

The procedure which is mentioned earlier is preceded in the proposed work, and it is implemented in the MATLAB environment, which is explained in depth in the upcoming sections. The security and efficient access control are obtained through this procedure.

4 Experimental Results

The experimentation is conducted in MATLAB. It is a programming language which is widely used in numerical and computing application. It is a computer environment follows a language that is designed to look similar to the notation used in linear algebra. To compare the improvement of the proposed methodology with the existing system with reference to the security level, different performance metrics has been taken into account. Those are as follows,

- Peak signal to noise ratio
- Mean squared error
- Security level

The proposed research methodology Secured and Attribute based User access control (SA-UAC) is compared with the existing methods namely confidential image data security based on encryption and watermark or CIDSEW [17], chaos encryption [18], Flash Digital Rights Management (DRM) [19]. The statistical evaluation is specified in the graphical formats.

The simulation results that are obtained are shown in the following Figures 2 and 11. Figure 2 show the sample of the input image which is used for embedding process. Figure 3 shows the sample of the embedding image. The outcomes of the binary segmented image

by MRFs are shown in Figure 4.

Figure 2. Input image

In the Figure 2, input image is shown which is taken as input to the proposed methodology for the secret message hiding.

Figure 3. Input image for embedding

In Figure 3, secret message is shown which is going to be hidden within the input image. This secret message will be hidden inside the input image using watermarking technique.

Figure 4. Binary segmented images

In Figure 4, segmented input image is shown in which region of interest part will be segmented and the secret message hiding will be performed.

The outcomes pertaining to the segmented color image by MRFs are denoted in Figure 5. The results concerning the color image which is watermarked are shown in Figure 6. Results of the color image that is encrypted by Attribute based encryption is denoted in Figure 7. Figure 8 illustrates the outcomes concerning the Salt and pepper attack added color image. Figure 9 shows the noise removed results of the Salt and pepper attack. Figure 10 shows the decryption image results of the input image. Figure 11 shows the decrypted results of embedded image.

Figure 5 specified the color segmented image which is performed after binary segmentation in order improve the watermarking process.

Figure 5. Color segmented images

In Figure 6, watermarked images are shown in which secret message shown in Figure 3 is hidden within the segmented input image.

Figure 6. Watermarked Images

The image which is encrypted is shown in Figure 7 where an image which is watermarked will be encrypted using attribute based encryption technique.

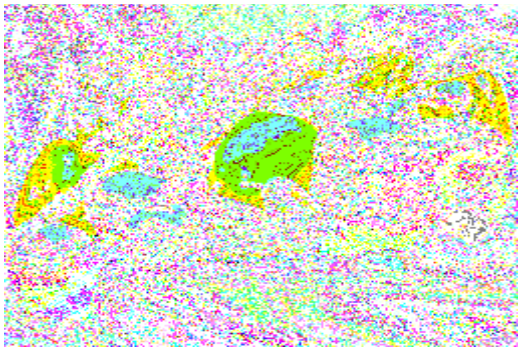

Figure 7. Encrypted images

In Figure 8, noise added image pertaining to salt and pepper is displayed which will be decrypted in order to gain the accurate image.

Figure 8. Salt and pepper attack image

In Figure 9, noise removed image is shown where the noise removal is performed at the received side before decryption.

Figure 9. Noise Removed Image

In Figure 10, received image which is to be decrypted in order to gain the secret message is shown.

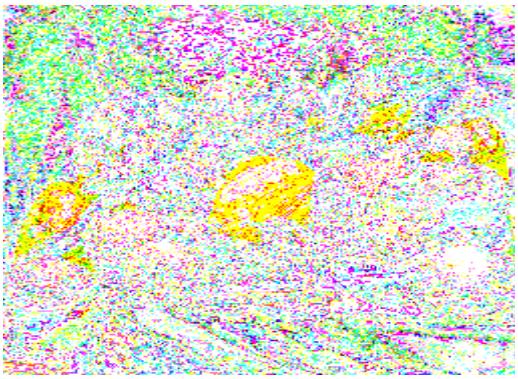

Figure 10. Decryption image

In Figure 11, decrypted watermarked image shown which reveals the secret message hidden inside the input images.

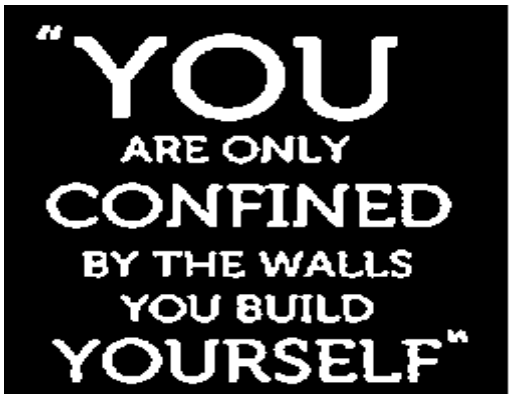

Figure 11. Decryption Of watermarked image

4.1 Peak Signal-To-Noise Ratio (PSNR)

PSNRor Peak Signal- To- Noise Ratio is often employed for measuring the quality of recreated image or video.

It denotes the proportion of the maximum possible power of an input image or video to the power of output image or video.

$$PSNR = 10\log_{10}(MAX_i^2 / MSE)$$

The results show that PSNR of the proposed Secured and Attribute based User access control (SA-UAC) scheme is better than the existing methods watermarking results confidential image data security based on encryption and watermark or CIDSEW.

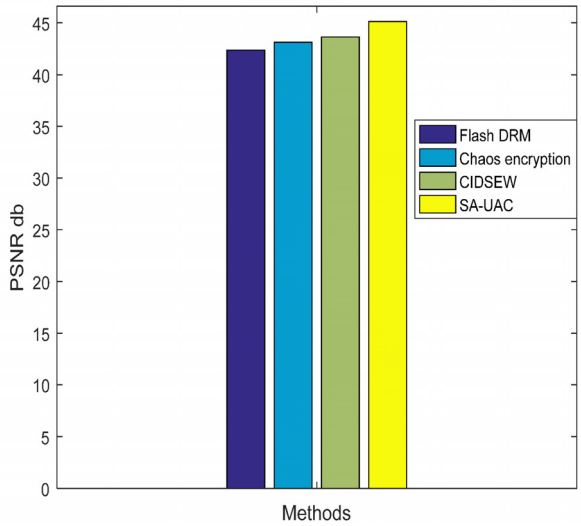

Figure 12. Experimental result against psnr comparison

From the Figure 12 it is proved that the proposed research work namely SA-UAC shows 14% performance improvement than the existing research method.

The proposed SA-UAC provides higher PSNR results of 44.78 dB, whereas other methods such as flash DRM, chaos encryption, and CIDSEW provides only 42.56 dB, 43.15 dB and 43.68 dB respectively.

4.2 Mean Square Error (MSE)

Mean square error or MSE pertaining to an estimator is for the calculation of the variation present between an estimator and the quantity's true value being calculated.

$$MSE = \frac{1}{m \times n} \sum_{k=0}^{m} \sum_{l=1}^{n} [f(k,l) - f'(k,l)]^2$$

Where,
f (k, l) - host video
f'(k, l) -embedded/ extracting image.

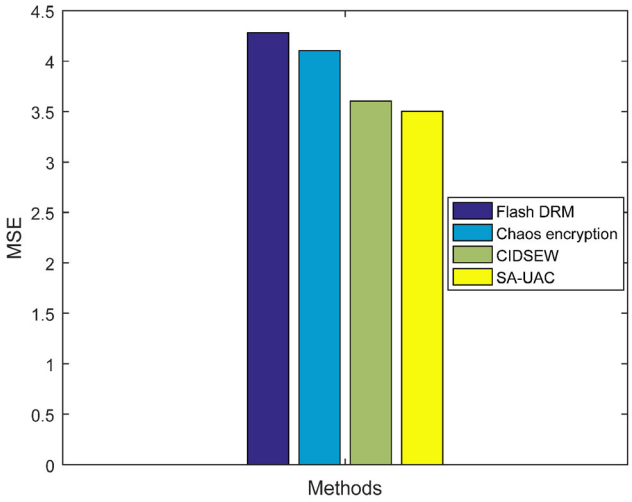

Figure 13. Experimental results of MSE comparison

The above experimental results prove that the proposed research work contains less MSE than the existing work. From the Figure 13 it can be illustrated that the existing method shows higher improvement by reducing in its MSE rate large than the present research methods.

It shows 85 % performance improvement than the existing method which is drastic improvement. The proposed SA-UAC provides lesser MSE results of 3.62 dB, whereas other method such as flash DRM, chaos encryption, and CIDSEW provides only 4.38, 4.21 and 3.75 respectively.

4.3 Security Level

The security of a symmetric cryptosystem is defined by a function of the length of the key. Here, we consider the length of the Key as an important aspect. The longer key length decreases the possibility of successful brute force attack. So, key length was selected as the first parameter in cryptographic algorithms. Key Length is a numeric metric which is generally expressed as a number of bits. The graph shows that the security level as key length increases.

The above Figure 14 confirms that as the key length increases the security level is also increasing gradually. Security level in the proposed work is higher than the existing methodology for varying key lengths. For example, for the key length of 512 bits, the security level of proposed work is 85 % and existing methodology is 75 %. The proposed SA-UAC provides higher security results of 85.00%, whereas other method such as flash DRM, chaos encryption, and CIDSEW provides only 67.00%,71.00%, and 75.00% respectively.

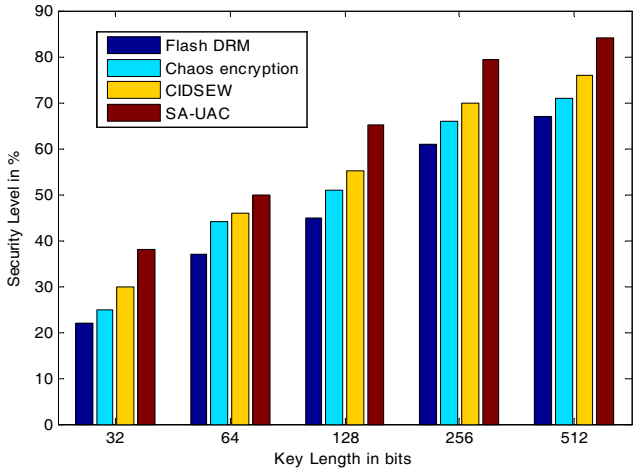

Figure 14. Key length vs. security level comparison

4.4 Correlation

Correlation is considered as any of the broad class of statistical relationships including dependence; however it mostly denotes the extent to which a linear relationship is present between two variables in regular usage.

The above Figure 15 results prove that the proposed research work contains high correlation than the existing work.

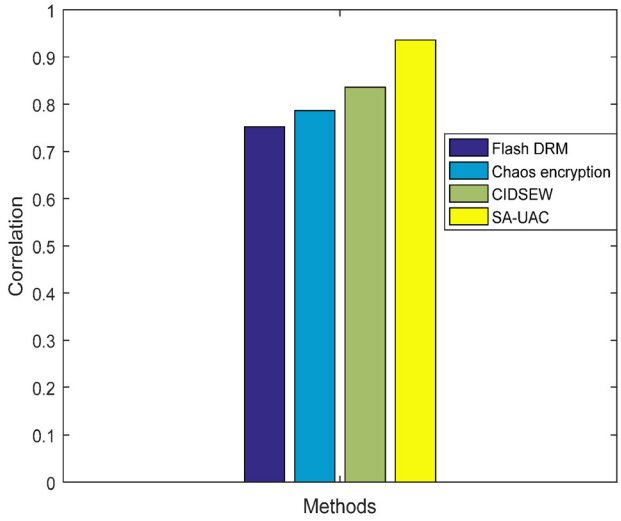

Figure 15. Correlation vs. methods

The correlation level of the proposed research methodology is considerably better in the proposed research method where it shows 27% performance improvement.

5 Conclusion and Future Work

The proposed work has introduced the novel approach namely Secured and Attribute based User access control (SA-UAC), which restricts the access control for the set of users, with respect to their access permission. Then for the security issue, sensitive parts of the confidential images are assured through segmenting the region of interest parts only from the whole image. In the proposed work, security and privacy are assured through cipher text policy based encryption that will restrict access permission based on the attributes. The experiment is implemented in MATLAB simulation environment with various parameters. The performance evaluation proves that the proposed work prompts to give a predominate result than the existing work. The proposed SA-UAC provides lesser MSE results of 3.62 dB, whereas other method such as flash DRM, chaos encryption, and CIDSEW provides only 4.38, 4.21 and 3.75 respectively. The present work is extended to any real time images and applications.

References

[1] T. Aichner, F. Jacob, Measuring the Degree of Corporate Social Media Use, *International Journal of Market Research*, Vol. 57, No. 2, pp. 257-275, March, 2015.

[2] S. Coulombe, G. Grassel, Multimedia Adaptation for the Multimedia Messaging Service, *IEEE Communications Magazine*, Vol. 42, No.7, pp.120-126, July, 2004.

[3] S. Alharthi, P. K. Atrey, Further Improvements on Secret Image Sharing Scheme, *ACM Proceedings of the 2nd Workshop on Multimedia in Forensics, Security and Intelligence*, Firenze, Italy, 2010, pp. 53-58.

[4] C. C. Chang, P. Y. Lin, Z. H. Wang, M. C. Li, A Sudoku-based Secret Image Sharing Scheme with Reversibility, *Journal of Communications*, Vol. 5, No. 1, pp. 5-12, January, 2010.

[5] C. Hu, X. Liao, D. Xiao, Secret Image Sharing Based on Chaotic Map and Chinese Remainder Theorem, *International Journal of Wavelets, Multiresolution and Information Processing*, Vol. 10, No. 3, pp. 1-18, May, 2012.

[6] J. Lang, A No-key-exchange Secure Image Sharing Scheme Based on Shamir's Three-pass Cryptography Protocol and the Multiple-parameter fractional Fourier Transform, *Optics Express*, Vol. 20, No. 3, pp. 2386-2398, January, 2012.

[7] E. Verheul, H. V. Tilborg, Constructions and Properties of k Out of n Visual Secret Sharing Schemes, *Designs, Codes and Cryptography*, Vol. 11, No. 2, pp. 179-196, May, 1997.

[8] S. R. Joshi, B. B. Amberker, N. V. Dharwadkar, Visual Cryptography for Gray-level Image Using Adaptive Order Dither Technique, *Journal of Applied Computer Science & Mathematics*, Vol. 3, No. 6, pp. 60-65, January, 2009.

[9] M. Naor, A. Shamir, *Advances in Cryptology Proceedings of Crypto 82*, Springer, 1995.

[10] L. Fang, B. Yu, Research on Pixel Expansion of (2, n) Visual Threshold Scheme, *International Symposium on Pervasive Computing and Applications*, Urumqi, China, 2006, pp. 856-860.

[11] T. Xiao-Qing, Two Kinds of Ideal Contrast Visual Cryptography Schemes, *International Conference on Signal Processing Systems*, Singapore, 2009, pp. 450-453.

[12] J. Crampton, A. Pinto, Attribute-based Encryption for Access Control Using Elementary Operations, *IEEE Computer Security Foundations Symposium (CSF)*, Vienna, Austria, 2014, pp. 125-139.

[13] N. Kaaniche, Laurent, M, Attribute Based Encryption for Multi-level access Control Policies, *SECRYPT International Conference on Security and Cryptography*, Madrid, Spain, 2017, pp. 67-78.

[14] R. Huang, V. Pavlovic, D. N. Metaxas, A Tightly Coupled Region-shape Framework for 3D Medical Image Segmentation, *IEEE International Symposium on Biomedical Imaging*, Arlington, VA, USA, 2006, pp. 426-429.

[15] V. Hu, Attribute Based Access Control (ABAC) Definition and Considerations, *National Institute of Standards and Technology*, pp. 1-4, March, 2004.

[16] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, J. Voas, Attribute-Based Access Control, *Computer*, Vol. 48, No. 2, pp. 85-88, Feburary, 2015.

[17] Z. Ma, J. Huang, M. Jiang, X. Niu, A Novel Image Digital Rights Management Scheme with High-level Security, Usage Control and Traceability, *Chinese Journal of Electronics*, Vol. 25, No. 3, pp. 481-494, May, 2016.

[18] A. Uhl, A. Pommer, Image and Video Encryption, *Advances in Information Security*, pp. 45-134, November, 2014.

[19] S. P. Mohanty, A Secure Digital Camera Architecture for Integrated Real-time Digital Rights Management, *Journal of Systems Architecture*, Vol. 55, No. 10-12, pp. 468-480, October, 2009.

Biographies

S. Lakshmi Narayanan obtained his bachelor's degree in Electronics and Communication Engineering from University of Madras, Chennai, India in the year 2002 and subsequently completed his master's degree in Communication Systems from SRM University Chennai, India in the year 2005. He has a total teaching experience of 15 years. Presently he is working as Assistant Professor at Sri Ramakrishna Engineering College, Coimbatore, India. He is pursuing his Ph. D at Anna University, Chennai, India. He has published two research papers and attended two conferences. His area of interests includes Image processing, Signal

Processing, Networking etc.

K. Sankaranarayanan born on 15.06.1952, completed his B.E. (Electronics and Communication Engineering) in 1975 and M.E. (Applied Electronics) in 1978 from P.S.G. College of Technology, Coimbatore under University of Madras. He did his Ph.D. (Biomedical Digital Signal Processing and medical Expert System) in1996 from P.S.G. College of Technology, Coimbatore under Bharathiar University. He has so far guided 19 Ph.D.s and presently guiding 02 research scholars for Ph.D. He has so far published 65 research papers in National and International Journals and around 60 papers in National and International conferences. His areas of interest include Digital Signal Processing, Computer Networking, Network Security, Biomedical Electronics, Neural Networks and their applications, and Opto Electronics. He has more than 40 years of teaching experience and worked in various Government and self financing Engineering colleges. At present he is working as DEAN (ECE) at P.A. College of Engineering and Technology, Pollachi, Coimbatore District, Tamil Nadu, India.

V. Vijaya Kumari, M.E., Ph.D., received her B.E. degree in Electronics and Communication Engineering from Bharathiar University in 1993. She also received her M.E. and Ph.D. degree from Anna University, Chennai. Currently she is working as a Professor in the Department of Electronics and Communication Engineering, Er. Perumal Manimekalai College of Engineering, Hosur. She carried out her research in the field of Medical Imaging. She has published 50 papers in International journals and conferences. Her research interest includes Medical imaging, Soft computing, Biometrics, Analog VLSI, Wireless Sensor Networks etc.