Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2025 SCPE. Volume 26, Issues 1, pp. 84–95, DOI 10.12694/scpe.v26i1.3574

SECURE DIGITAL DATA VISUAL SHARING SCHEMES IN MULTI-OWNER PUBLIC CLOUD ENVIRONMENT APPLICATIONS

CHEKKA RATNA BABU* AND B. RAVEENDRA BABU †

Abstract. The use of cloud computing for storing and processing cyber data via the internet has grown widespread in the field of cyber security. Ensuring the secure sharing of cyber data, including texts, images, audio, and video, over the cloud is paramount. However, cloud computing encounters significant challenges concerning cyber data security, authentication, and privacy. The prevailing approaches to data security encounter challenges such as the generation of intricate keys, intensive computation for large keys, and susceptibility to attacks by intruders. Scalability presents its own set of obstacles in maintaining cyber data privacy and ensuring secure communication. A significant privacy concern arises from the frequent changes in membership and data sharing among multiple owners. This paper introduces a novel approach to secure data sharing within data centres by proposing a scheme that employs Private Key Dynamic Visual Cryptography (PK-DVC), Multiple Key Encryption Visual One-Time Pad (MK-VOTP), and visual steganography for encoding and decoding. MK-VOTP is used for data encryption, facilitating data owners' encryption via utilising their identity with supplementary security features. Subsequently, the encrypted data is kept in the cloud, guaranteeing heightened security protocols. Visual steganography is employed for further authentication purposes. Decrypting the original data requires users who fulfil the encrypted properties. This increases security and reduces critical size, allowing several authenticated owners to share data without conflicts. Combining all shares recreates the original picture.

The approach described in the paper sounds innovative and addresses several key challenges in ensuring secure data sharing within data centers, particularly in the context of cloud computing.The proposed scheme main components are *Private Key Dynamic Visual Cryptography (PK-DVC),Multiple Key Encryption Visual One-Time Pad (MK-VOTP)*, and *Visual Steganography*.These three components plays important role in further authenticating the encrypted data or providing additional security measures beyond encryption.By combining these techniques, the proposed scheme aims to provide robust security for sharing cyber data in cloud environments. The use of dynamic keys, multiple encryption layers, and steganography can enhance data security, making it challenging for intruders to access or decipher sensitive information.

Key words: Multi-Owner, Encryption, Visual Cryptography, Decryption, Cloud Computing, Visual Steganography

1. Introduction. Since 2007, the IT industry and academics have focused on cloud computing. The idea involves assigning services in a "cloud," a network of devices and resources linked via the Internet, to seamlessly offer more flexible services to consumers. Data storage, an essential component of cloud computing, presents new issues in developing safe and reliable storage and access methods among cloud service providers [5]. Given cloud computing's inherent openness, cloud data storage must be secured [6].In Figure.1 Multiowner – Cloud Architecture Access control is crucial in cloud-based systems due to data accessibility.

However, ensuring the security and privacy of data stored in the cloud presents significant challenges. While data encryption offers protection, concerns arise when cloud servers possess decryption keys and manage user accessibility rights, particularly for sensitive records like administrative documents (e.g., bills and ID cards)[5]. Additionally, as users increasingly outsource storage and computing needs to remote servers, often untrusted, privacy issues escalate, including the sensitivity of keywords transmitted in queries and the retrieved data, requiring concealment. Consequently, security and privacy emerge as paramount concerns. Traditional network security and privacy mechanisms need to be revised or address data storage and outsourcing complexities. Maintaining the integrity and confidentiality of stored digital data identities becomes a significant challenge external storage solutions pose [6]. Dynamic visual cryptography and steganography techniques mitigate these risks and preserve data privacy and authentication in the cloud.

Dynamic Visual Cryptography: The dynamic visual cryptography scheme offers a robust approach to encrypting confidential documents or images by partitioning them into distinct segments. One noteworthy

*Acharya Nagarjuna University, Guntur, India (chekka.ratnababu@gmail.com)
†Accreditations & Recruitment, Vishnu Group of Institutions, Hyderabad & Bhimavaram, India (rbhogapathi@yahoo.com)

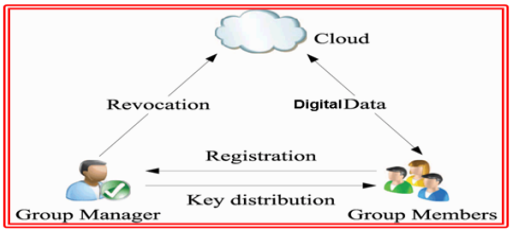


Fig. 1.1: Multiowner - Architecture

characteristic of visual cryptography [7][8][9] is the ability to visually decipher the secret picture by superimposing shares, hence obviating the need for intricate computational processes. Exploiting this property, a third party can easily reconstruct the secret image if the shares are transmitted sequentially over the network. This approach involves encrypting visually generated image shares using Private Key Encryption, with the primary objective of achieving a high level of security. Unlike previous systems where only a single user could access the data, this system enables multiple users to access the same data. Moreover, it utilizes more minor keys than the larger keys previously employed. Addressing the paramount concern of security in data sharing over the cloud, this system aims to mitigate associated risks effectively.

2. Relade Work. Data undergoes encryption before outsourcing, resulting in the service provider receiving encrypted data. Consequently, this data is perceived as useless or lacking in meaning. However, the responsibility for managing access control policies, encrypting and decrypting data, and managing cryptographic keys falls on the client [10]. Adding to the user's burden and sharing it increases hazards. Data shared among several users requires more encryption flexibility to accommodate group members, enable key management, and enforce access control regulations to protect data confidentiality. Outsourced data owners have extra constraints when sharing data with many consumers.

Public key encryption encounters difficulties when implemented in cloud environments, with numerous users needing file access. Sana et al. introduced a lightweight encryption algorithm in their study cited as [11], melding symmetric encryption for file encryption and asymmetric encryption for crucial distribution to tackle these challenges. Nonetheless, this approach has drawbacks, including complexities in key management and the necessity for precise file access control, as noted in [12]. Furthermore, the solution's flexibility and scalability could be improved. Encryption and decryption [29] methods must be implemented whenever a user leaves a group to prevent unauthorised access to data.

Shamir established the concept of identity-based encryption [13]. This encryption method involves data owners encrypting their data by providing the identity of the authorised entity responsible for decrypting it. The decryption entity's identity must correspond to the one designated by the owner, therefore obviating the need for key exchange.

Attribute-based encryption (ABE) is a cryptographic technique that establishes user identification [32] using a characteristic collection. These qualities are then used to build a secret key and establish the access structure for access control. This approach integrates encryption with access control, allowing for data confidentiality and sharing among groups of users. In [14], fuzzy identity-based encryption (FIBE), a variant of ABE, was proposed several years after IBE. In FIBE, a group of attributes collectively identifies an individual's identity. The data owner encrypts the data, and only individuals possessing attributes that overlap with those specified in the ciphertext can decrypt it.

Ostrovsky's technique [15] introduces a method that enables the implementation of non-monotonic access structures, which may accommodate both positive and negative qualities. Nevertheless, this technique leads to a rise in the size of the ciphertext and the key and the accompanying time expenses for encryption and decryption. On the other hand, Key-Policy Attribute-Based Encryption (KP-ABE) exhibits a linear growth in the ciphertext size as the number of related characteristics increases.

An algorithm has been devised to guarantee a consistent ciphertext size irrespective of the number of characteristics while accommodating non-monotonic access patterns. Nevertheless, the dimensions of the critical

exhibit a quadratic growth pattern as the number of factors increases. Cypher Text Policy Attribute-Based Encryption (CP-ABE) was developed to address this problem [16]. Nevertheless, it is essential to acknowledge that CP-ABE often entails more expenses than KP-ABE.

Cybersecurity between Users W. Chen and Wang's Mobile Media Cloud [17] secured multimedia data across users' clouds. The system used DCT RS code watermarking, picture concealing, and secret sharing. Its advantages were strong security, user-friendliness, media quality, and low overhead. One downside was that picture data was limited to one carrier. This constraint is overcome by dividing the picture into shares and transmitting the data over carriers.

S, Chauhan, and Vats suggested Threshold Cryptography-Based Data Security in Cloud Computing [18] to protect communication between Data Owners (DO), Managed Service Providers (MSP), and cloud customers and cyber data access. The system used Diffie-Hellman, threshold cryptography, and MD5. Its benefits were reduced keys and improved data security, confidentiality, integrity, and performance. Diffie-Hellman algorithm computing power was a system downside. To address this issue, the system replaced the Diffie-Hellman algorithm with MK-VOTP, a lightweight encryption method, to achieve efficient encryption and decryption without requiring extensive computational power.

The goal of the Digital Image Sharing by Diverse Image Media [19][30] method proposed by Lee and Chiu was to partition photographs into several shares safely. The system utilized techniques such as the NSS algorithm and encoding algorithms. Its benefits encompassed user-friendliness, high security, quality images, and low-risk transmission. However, a drawback of the system was generating noise-like shares during the process. Mukherjee and Ghoshal presented "Steganography-based Visual Cryptography" [20] to bolster image security by integrating Steganography with Visual Cryptography (VC), a method where data is concealed within another image. The system employed techniques such as cryptography and steganography. Its advantages included heightened security, authentication, integrity, and reduced computational overhead. However, a potential drawback could be a decline in image quality. In this study, efforts were made to address weaknesses such as poor image quality and noisy generated shares while enhancing privacy, authentication, and robustness.

3. Proposed Work. Securing information to restrict access solely to authorized individuals has been a longstanding practice. However, this pursuit encounters challenges in both physical and digital domains. Even well-protected information remains susceptible to theft or unintended misuse in the tangible world. Similarly, the cyber realm faces comparable obstacles, often resorting to container-based encryption for safeguarding. The analogy of lock-and-key security persists in digital landscapes, where data integrity hinges on robust encryption techniques. Within cloud environments[21], digital identity is the cornerstone of adaptable data security. Digital identity encompasses diverse attributes defining an individual, thereby presenting risks of identity theft. Consequently, upholding the confidentiality of digital identities is crucial, not only for security but also for privacy.

For instance, email represents a typical scenario of multi-owner privacy data[2]. When two individuals exchange an email, the content becomes a shared privacy concern and which is shown in Figure 3.1. The contents should not be disclosed without either party's consent [3][4]. Nevertheless, given that the email is owned by both the correspondent and the recipient[1], they each possess the authority to forward it autonomously. Forwarding entails the inherent danger of revealing the confidential data of the other proprietor.

The Online Patient Health Record System (OPHRS) looks promising for online patient health information exchange. Patients may manage, regulate, and share their health data with other users and doctors. When OPHRS is semi-trusted to a third-party server, issues about unauthorised access, privacy breaches, and security vulnerabilities develop, creating substantial problems in a multi-owner cloud environment. A secure cloud-based OPHRS architecture addresses these issues. MK-VOTP and visual steganography enable safe OPHRS sharing across several users in this system.

The proposed system is a collaborative platform to facilitate secure image sharing among multiple users on cloud infrastructure. Given the inherent limitations of cloud services in ensuring security, confidentiality, and integrity, this system employs Visual Cryptography[22][23] to distribute image components among group members. Each segment of the image undergoes encryption and decryption procedures using dynamic visual cryptography. Visual steganography[24][25] is integrated as an additional protective layer to fortify security measures and validate authentication. Traditionally, images were transmitted as single carriers, leaving them

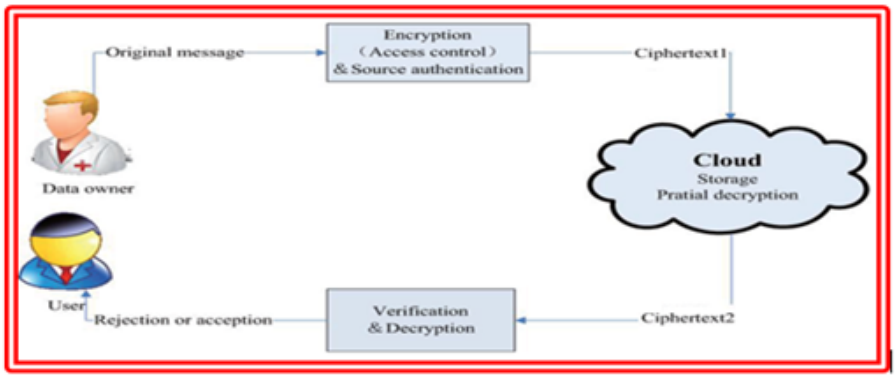


Fig. 3.1: Cloud Environment Encryption/Decryption

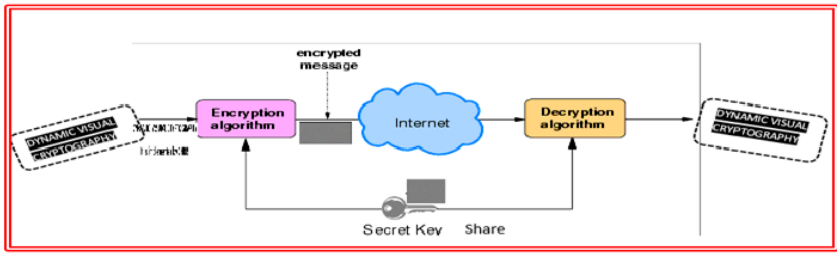


Fig. 3.2: Private Key Dynamic Visual Encoding/Decoding

vulnerable to loss. A single image is fragmented into multiple shares and carriers to mitigate this risk. Cloud service users must understand computing environment obligations and security and privacy concerns. Thus, the suggested system provides cloud computing solutions for organisational security and privacy. The ultimate aim of the proposed system is to achieve real-time image transfer to authenticated users. By consolidating the image shares, the complete image is reconstructed. Any unauthorized alterations to the image trigger access restrictions for users. The system effectively reduces the likelihood of data tampering or unauthorized access through multiple encryption and decryption operations.

3.1. Private key Dynamic Visual Cryptography Encryption. Dynamic Visual Cryptography [26-28] is an exceptional encryption technique designed to hide information within images, enabling decryption by human vision with the correct key image. This method employs two transparent images: one containing random pixels (the key) and the other holding the secret information. Retrieving the hidden data from either image alone is unfeasible; both are essential to reveal the concealed information. When the random image comprises genuinely random pixels, it functions similarly to a One-time Pad system, delivering encryption highly resistant to decryption.All algorithmic steps are revealed in Figure 3.2.

3.2. Multiple Key Encryption Visual One–Time Pad. MK-VOTP is suggested for cloud owner/user authentication. Figure 3.3 solution allows several owners to authenticate to the cloud server using multi-level security. Several owners may obtain shares from the group management and utilise the token several times.

Since the cloud cannot guarantee security, secrecy, or integrity, this multi-owner solution lets anybody safely transmit photos to numerous owners on the cloud. Each group member distributes a portion of the picture using Dynamic Visual Cryptography [33][34]. Dynamic visual cryptography encrypts and decrypts each picture sharing. Steganography will be used to improve security and check for sharing manipulation. Organisations and people using cloud services must comprehend computing environment obligations and security and privacy implications. Therefore, the suggested method ensures that cloud computing solutions meet organisational

Algorithm 1 Private Key Dynamic Visual Encoding/Decoding

a.Generate Private Key(imgKey):

```
Input:The given input consists of a Gray-Scale Image (GI) with t1 x t2 pixels dimensions.
 The basis matrices C0 and C1 have sizes of n x m.
Output: Securely generates a new Key Image
Step 1: First, create a fully transparent white pixel grey scale (GI) image with size t1 × t2 pixels
Step 2:  an image to transform into a key by turning its black pixels into 3/4 pixel blocks
Step 3:  an image to transform into a key by turning its white pixels into 2/4 pixel blocks
            (which itself are randomly determined).
Step 4: Non-white pixels are treated as if they were black.
Step 5: Fully white image for truly random key
```

b.Encoding(imgKey, imgSrc) Pseudo Code:

```
Step 1:BufferedImageencryptedImage=new BufferedImage(key image.getWidth(),key image.getHeight(),
           BufferedImage.TYPE_INT_ARGB);
Step 2: for (int y = 0; y < encryptedImage.getHeight(); y += 2) {
Step 3: for (int x = 0; x < encryptedImage.getWidth(); x += 2) {
Step 4:   if (sourceImageRes.getRGB(x, y) == Color.BLACK.getRGB()) {
Step 5:   if (keyImage.getRGB(x, y)>>>24 == 0)
          encrGraphics.fillRect(x, y, 1, 1);
          if (keyImage.getRGB(x + 1, y)>>>24 == 0)
          encrGraphics.fillRect(x + 1, y, 1, 1);
      if (keyImage.getRGB(x, y + 1)>>>24 == 0)
          encrGraphics.fillRect(x, y + 1, 1, 1);
     if (keyImage.getRGB(x + 1, y + 1)>>24 == 0)
          encrGraphics.fillRect(x + 1, y + 1, 1, 1);
      } else {
      if (keyImage.getRGB(x, y) == Color.BLACK.getRGB())
          encrGraphics.fillRect(x, y, 1, 1);
          if (keyImage.getRGB(x + 1, y) == Color.BLACK.getRGB())
          encrGraphics.fillRect(x + 1, y, 1, 1);
   if (keyImage.getRGB(x, y + 1) == Color.BLACK.getRGB())
          encrGraphics.fillRect(x, y + 1, 1, 1);
   if (keyImage.getRGB(x + 1, y + 1)== Color.BLACK.getRGB())
          encrGraphics.fillRect(x + 1, y + 1, 1,  1);}}}
Step 6: return encryptedImage;
```

c. Decoding(keyImage, overlayImage) Pseudo Code:

```
Step 1: BufferedImage cleanImage = new
        BufferedImage(overlayImage.getWidth() / 2,  overlayImage.getHeight() / 2 , BufferedImage.TYPE_INT_ARGB);
Step 2: for (int yOverlay = 0, yClean = 0; yOverlay <overlayImage.getHeight(); yOverlay += 2,  ++yClean)
Step 3: for (int xOverlay = 0, xClean = 0; xOverlay <overlayImage.getWidth(); xOverlay += 2,  ++xClean) {
             int rgbFirstPixel = overlayImage.getRGB(xOverlay, yOverlay);
Step 4: if (rgbFirstPixel >>>24 != 0 &&
        overlayImage.getRGB(xOverlay + 1, yOverlay) >>>24 != 0  &&
         overlayImage.getRGB(xOverlay, yOverlay + 1) >>>24 != 0   &&
         overlayImage.getRGB(xOverlay + 1, yOverlay + 1) >>>24 != 0) {
cleanGraphics.setColor(new Color(rgbFirstPixel, true));
cleanGraphics.fillRect(xClean, yClean, 1, 1);
}}}
Step 5: return cleanImage;
```

security and privacy needs.

The ultimate result of the suggested system is the successful real-time delivery of the secret picture to the authorised users. The original image will be created by merging the shared portions of the image. If any manipulation is performed on the picture, the user's ability to access the image will be limited. The picture undergoes various encryption and decryption processes, making tampering with or hijacking the data challenging. Therefore, if an unauthorised user attempts to get access to the confidential picture, they will be unable to do so if any malicious user tampering occurs with the secret image since it may be discovered via steganography. If any user's private key is absent, the original picture will remain inaccessible to all users.

3.3. Secure Secret Share Visual Steganography. A network of interconnected bank branches provides cloud banking services [37]. Cloud bank customers can access their assets and carry out basic transaction

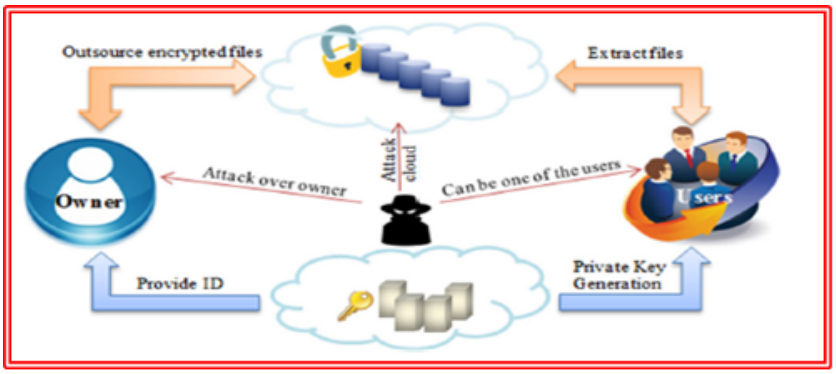


Fig. 3.3: Multiple Key Encryption Visual One–Time Pad

Algorithm 2 Algorithm Multiple Key Encryption Visual One–Time Pad Pseudo Code:

```
EncDoubledKey(Image newImage1, Image newImage2, int height, int width, int n){
Step 1: m_enc2 = new Enc2_2(height, width, n);
Step 2: m_loadingImage1 = newImage1;
  m_loadingImage2 = newImage2;
Step 3: this.initEncrypt();
       }
              initEncrypt(){
         Step 3.1: m_enc2.doPermutation();
         Step 3.2: m_enc2.setImage(m_loadingImage2);
         Step 3.3: m_enc2.encrypt();
                        //this.doPermutation();
         Step 3.4: m_Cblack = m_enc2.m_Cblack;
         Step 3.5: m_Cwhite = m_enc2.m_Cwhite;
         Step 3.6: this.setImage(m_loadingImage1);
         Step 3.7: this.encrypt();
         return true;  }
```

activities from any member cloud network bank branch office. One of the primary challenges encountered in cloud banking services is the integrity of the members. The authentication of information in the cloud banking industry is a significant challenge due to the occurrence of SQL Injection hacking attacks on bank databases. To address the challenges associated with authentication, this study proposes a method that utilises image processing techniques to secure secret sharing using visual steganography. The present study introduces a novel approach to embedding a customer's PIN using secure secret share visual steganography. While many existing steganography methods rely on three or four adjacent pixels over a single pixel, the secure secret share visual steganography technique [35][36] offers the advantage of utilising up to eight adjacent neighbours. This allows for a gradual increase in value, which can then be divided into multiple segments. The quantity of shares to be generated is contingent upon the specific plan the financial institution selects. After creating two shares, one share is recorded in the bank database, and the client retains the second share. The consumer needs to ensure the presentation of their share throughout all transactions. The original picture is obtained by stacking this share with the first share. The decoding process extracts the concealed pin number upon acknowledging or rejecting the output, verifying the customer's identity.

Multi – Owner Public Cloud Environment is a conceptual model that outlines the cloud application, behavior, and aspects, as depicted showin Figure 3.4.

Figure 3.5.(a) shows the logic flow to generate shares by using MK-VOTP algorithm and visual Stenography algorithm. If both the keys (private key 1 and private key 2) are same, cloud member authenticity may be

Algorithm 3 Visualstegnography Algorithm

```
Step 1: BufferedImage keyFromInitialImage = Crypting.generateKey(imgFirst);
Step 2: BufferedImage secondImageCanvas =
        new BufferedImage(width*2, height * 2, BufferedImage.TYPE_INT_ARGB);
Step 3: for (int y = 0; y < height; ++y) {
        for (int x = 0; x < width; ++x) {
        int newX = x * 2;
        int newY = y * 2;
        int pixelRGB = imgToHide.getRGB(x, y);
        boolean targetShouldBeBlack = (pixelRGB >>> 24 != 0); // Check transparency
        pixelRGB = secondImageCanvas.getRGB(x, y);
        boolean secondImagePixelIsBlack = (pixelRGB >>> 24 != 0);
Step 4: int blackPixelsToSet = secondImagePixelIsBlack ? 3 : 2;
Step 5: boolean skipFirst = !targetShouldBeBlack;
        for (int minix = 0; minix < 2; ++minix) {
        for (int miniy = 0; miniy < 2; ++miniy) {
        int firstPixelRGB = keyFromInitialImage.getRGB(newX + minix, newY + miniy);
        boolean isFirstPixelWhite = (firstPixelRGB != Color.BLACK.getRGB());
        if (isFirstPixelWhite) {
          if (skipFirst) {
            skip first = false;
            newPixels[minix][miniy] = Boolean.FALSE;
            continue;
          }
          newPixels[minix][miniy] = Boolean.TRUE;
          --blackPixelsToSet; } } } } }
```

Fig. 3.4: Proposed Method Cloud Multi Owner Security Flow Diagram

granted and if both are not same, admin can decide that the share produced by cloud member is fake and can be rejected. In Cloud Member Registration/Verification to register [Figure 3.5.(b)] the cloud member and Verify (Figure. 3.5.(c)) the correct cloud member or not.

4. Experiments and Results. The outcome of the system entails the retrieval and creation of the first picture on the customer's end via the accumulation of the shares held by the participating consumers. The agent sends the image, which is then subjected to Visual Cryptography. This involves splitting the image into n shares. The sensitive data is then encrypted using private critical dynamic visual cryptography and a one-time multiple-key encryption visual pad. The encoded and decoded shares are then authenticated. Finally, Visualstegnography is used to authenticate the customers .The Simulation results shown in from Figure. 4.1a to Figure 4.2c step by step in sequence order.

The efficiency of Visual cryptosystem depends on the quality of the reconstructed image. The important parameters of proposed VC scheme are pixel expansion(m), which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image and contrast (α), which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image. Generally, smaller the value of m will reduce the loss in resolution and greater the value α of will increase the quality of the reconstructed image. As mentioned above if 'm' is decreased, the quality of the reconstructed image will be increased but security will be a problem The secret

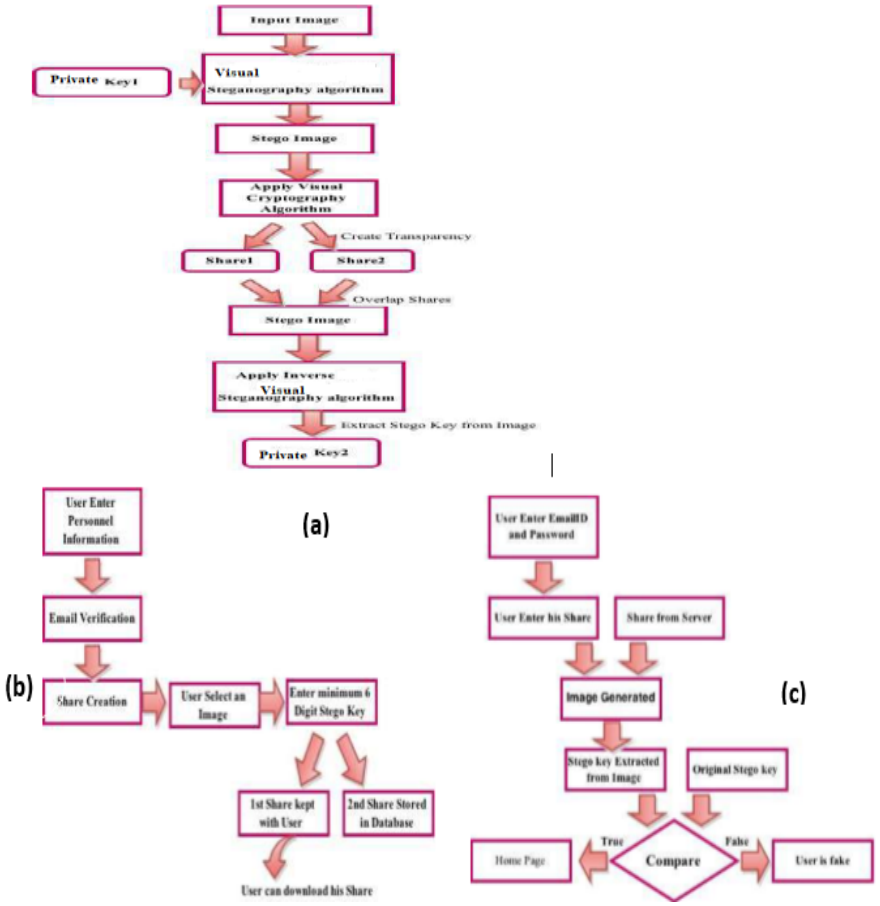
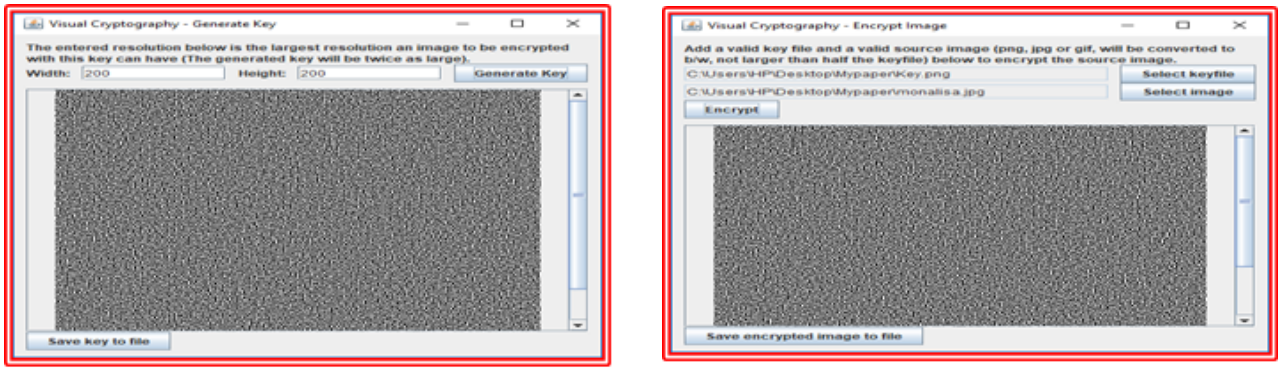


Fig. 3.5: Proposed Method Cloud Multi Owner Security Flow Diagram

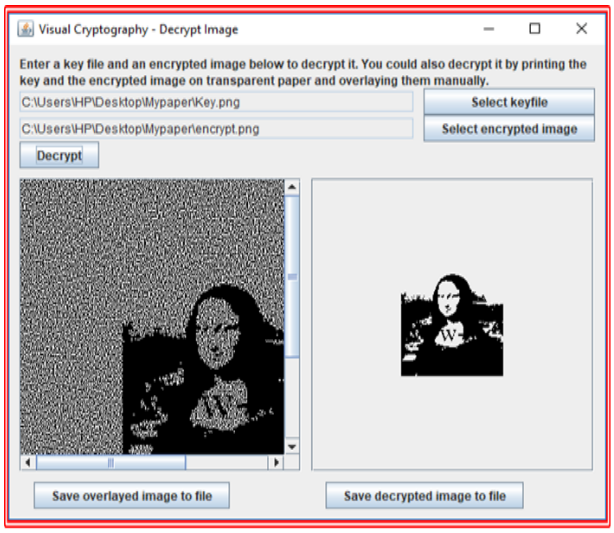


(a) Generate Key

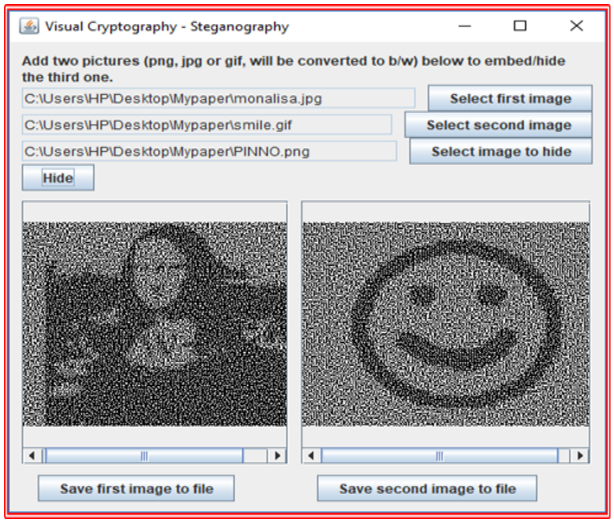
(b) Private Key Encoding

Fig. 4.1: Generate Key and Private Key Encoding

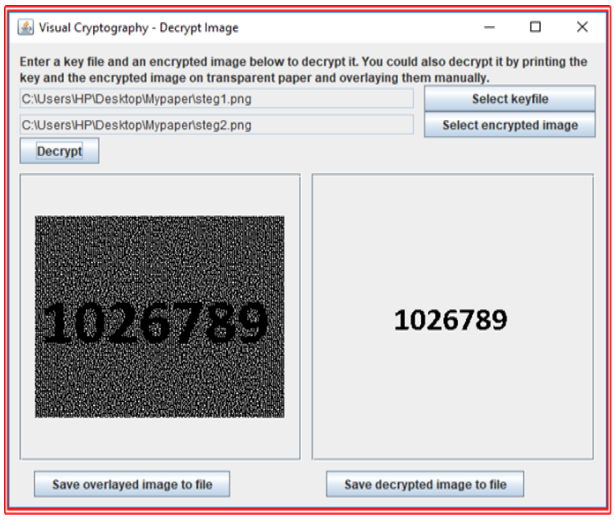
share or reconstructed image generated from the original image (Figure 4.3a) is shown in Figure 4.2b, the



(a) Private Key Decoding



(b) Visualstegnography embed

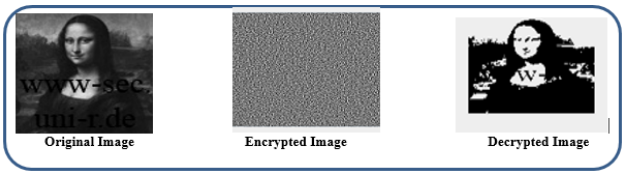


(c) Visualstegnography (overlayed and Descrypted Image)

Fig. 4.2

corresponding ownership share is shown in Figure 4.2c, and the stacked result of Figure 4.2a and Figure 4.2b is illustrated in Figure 4.2c. In the Secrete Share the ratio of block pixels to white pixels is 50.21 to 49.79,Which reflects the central limits statement. In addition, two common similarity measurements are introduced to evaluate the proposed cloud membership protection scheme.One is the peak signal-to-noise ratio (PSNR) used to evaluate the similarity of two grey-level images

$$PSNR = 10 \times \frac{log(255)^2}{MSE}$$



(a)

(b)

Fig. 4.3: Visualstegnography (PSNR/SSIM)

Table 4.1: Quality measures of the images

(a) For Figure 4.3a

Image	**SSIM index**	**PSNR**
Original Image	1	18.49dB
Encrypted Image	0.0004	31.79 dB
Decrypted Image	0.90	20.33 dB

(b) For Figure 4.3b

Image	**SSIM index**	**PSNR**
Original Image	1	19.54 dB
Encrypted Image	0.0003	33.38 dB
Decrypted Image	0.89	21.22 dB

where

$$MSE = \frac{1}{M1 \times M2} \times \sum_{i=1}^{M1} \sum_{j=1}^{M2} (hij - (hij^1)^2)$$

hij denotes a pixel color of the original image,and h1ij denotes a pixel color of the attacked image,$M1 \times M2$ is the size of the image. Another parameter is the Structural Similarity (SSIM) index for measuring the quality between two images. The SSIM index can be viewed as a quality measure of one of the images being compared provided the other image is regarded as of perfect quality. The quality measures are calculated between the original image and the encrypted/decrypted image. Table 4.1a and Table 4.1b shows the quality measures of the images in Figure 4.3a and in Figure 4.3b.

5. Conclusion. This paper explores a growing trend in implementing multiple security techniques to manage security risks on the cloud effectively, thus unlocking the full potential of cloud computing. The proposed approach significantly contributes to cloud security and privacy, focusing on authentication and protecting image copyright and multimedia data confidentiality. Visual cryptography is employed for encrypting, concealing, and sharing information in image form, ensuring that the information is only visible to the human eye upon decryption with the correct key. Visual steganography embeds secret information and various features into original images, facilitating the identification of ownership of modified images and addressing issues related to tampering and verification. Sensitive data is secured using dynamic visual cryptography with private keys and Multiple Key Encryption Visual One-Time Pad methods. Users may encrypt their data with their identity and other security features and save it in the cloud. Additionally, visual steganography improves authentication .

Moreover, the scheme seems to address scalability concerns by allowing multiple authenticated owners to share data without conflicts, thus ensuring secure communication even in dynamic environments with frequent

changes in membership and data sharing.

Overall, this approach appears promising in mitigating the challenges associated with cyber data security, authentication, and privacy in cloud computing environments. However, its effectiveness would need to be evaluated through rigorous testing and analysis to ensure its practical viability and resilience against potential attacks.

REFERENCES

[1] Yi Ren, Fangquan Cheng, Zhiyong Peng, Xiaoting Huang, Wei Song. "A privacy policy conflict detection method for multi-owner privacy data protection", *Electronic Commerce Research*, 2010.

[2] F. Koufogiannis and G. J. Pappas, "Multi-owner multi-user privacy," *IEEE 55th Conference on Decision and Control (CDC)*, Las Vegas, NV, USA, pp. 1787-1793, 2016.

[3] Saikiran Ellambotla, Dr. Anubarti, Dr. Md.Ateeq Ur Rahman. "Cloud Computing Data Group Distribution and Restricted Distribution with Multi Owner", *International Journal of Engineering Science Invention (IJESI)*, Volume 8, Issue 11, PP 37-45, 2019.

[4] X. Liu, Y. Zhang, B. Wang and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1182-1191, June 2013.

[5] Abo-alien, A., Badr, N.L., Tolba, M.F. "Data Storage Security Service in Cloud Computing: Challenges and Solutions", *Multimedia Forensics and Security. Intelligent Systems Reference Library*, vol 115. Springer, Cham. 2017.

[6] Paul, V., Mathew, R. (2020). "Data Storage Security Issues in Cloud Computing". In: Pandian, A., Palanisamy, R., Ntalianis, K. (eds) *Proceeding of the International Conference on Computer Networks, Big Data and* IoT (ICCBI - 2019). ICCBI 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 49. Springer, Cham.

[7] S. -J. Lin and W. -H. Chung, "A Probabilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 197-207, Feb. 2012

[8] Chitra, K., Prasanna Venkatesan, V. (2020). "A Dynamic Security Model for Visual Cryptography and Digital Watermarking". In: Pandian, A.P., Senjyu, T., Islam, S.M.S., Wang, H. (eds) Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018). ICCBI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 31. Springer.

[9] Rajkumar Kushwaha, Ankit Gajakosh, Prasanna More, Manjusha Shelke, Nilima Patil. "Visual Cryptography", International Journal of Creative Research Thoughts Volume 6, Issue 1, pp 584-587, 2018.

[10] Zhang, R., Wang, J., Song, Z. et al. "An enhanced searchable encryption scheme for secure data outsourcing". Sci. China Inf. Sci. 63, 132102 ,2020

[11] Sana Belguith, "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm", Conference: ICAS 2015: The Eleventh International Conference on Autonomic and Autonomous Systems

[12] K. Marimuthu, D. G. Gopal, K. S. Kanth, S. Setty and K. Tainwala, "Scalable and secure data sharing for dynamic groups in cloud," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, Ramanathapuram, India, 2014, pp. 1697-1701.

[13] Sahai, A., Waters, B. "Fuzzy Identity-Based Encryption". In: Cramer, R. (eds) Advances in Cryptology – EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin.

[14] Chen, Y., Jiang, Z.L., Yiu, S.M., Liu, J.K., Au, M.H., Wang, X. (2015). "Fully Secure Ciphertext-Policy Attribute-Based Encryption with Security Mediator". In: Hui, L., Qing, S., Shi, E., Yiu, S. (eds) Information and Communications Security. ICICS 2014. Lecture Notes in Computer Science(), vol 8958. Springer, Cham.

[15] C. -J. Wang and J. -F. Luo, "A Key-policy Attribute-based Encryption Scheme with Constant Size Ciphertext," 2012 Eighth International Conference on Computational Intelligence and Security, Guangzhou, China, 2012, pp. 447-451.

[16] H. Wang, S. Wu, M. Chen and W. Wang, "Security protection between users and the mobile media cloud," in IEEE Communications Magazine, vol. 52, no. 3, pp. 73-79, March 2014.

[17] S. K. Saroj, S. K. Chauhan, A. K. Sharma and S. Vats, "Threshold Cryptography Based Data Security in Cloud Computing," 2015 IEEE International Conference on Computational Intelligence and Communication Technology, Ghaziabad, India, 2015, pp. 202-207.

[18] K. -H. Lee and P. -L. Chiu, "Digital Image Sharing by Diverse Image Media," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 88-98, Jan-2014.

[19] Mukherjee, R., and Ghoshal, N. (2013). Steganography Based Visual Cryptography (SBVC).

[20] Jon Henning "Exploring Real-World Cybersecurity Examples", Coordinated Business Systems Blog, Aug 31, 2023.

[21] Murad, S.H., Rahouma, K.H. (2022)." Hybrid Cryptography for Cloud Security: Methodologies and Designs". Digital Transformation Technology.

[22] Ms.Vaishnavi S. Kshirsagar1, Prof. N. M. Sawant, " Privacy Protection for Cloud Based Online Transaction Using Steganography and Visual Cryptography", International Journal of Innovations in Engineering and Science, Vol. 8, No. 5, 2023, PP. 42-44.

[23] Zadiraka, V.K., Kudin, A.M. "Cloud computing in cryptography and steganography". Cybern Syst Anal 49, 584–588 (2013).

[24] Adee, Rose, and Haralambos Mouratidis. 2022. "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography" Sensors 22, no. 3: 1109.

[25] Devika, K.D., Saxena, A. "Dynamic Authentication Using Visual Cryptography". In: Satapathy, S.C., Lin, J.CW., Wee, L.K., Bhateja, V., Rajesh, T.M. (eds) Computer Communication, Networking and IoT. Lecture Notes in Networks and

Systems, vol 459. Springer, Singapore.
[26] Palevicius, A., Janusas, G., Ragulskis, M., Palevicius, P., Sodah, A. (2018). "Design, Analysis, and Application of Dynamic Visual Cryptography for Visual Inspection of Biomedical Systems". In Bonča, J., and Kruchinin, S. (eds), Nanostructured Materials for the Detection of CBRN. NATO Science for Peace and Security Series A: Chemistry and Biology. Springer, Dordrecht.
[27] Ch.RatnaBabu, M.Sridhar and Dr.B. RaveendraBabu, "Information hiding in greyscale images using pseudo-randomized visual cryptography algorithm for visual information security", Proceedings of IEEE International Conference on Information Systems and Computer Networks (ISCON), at Gala University, Matura, ISBN:978-1-4673-5987-0, 9-10 March 2013, pp.195 – 199.
[28] Sultan Aldossary and William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", International Journal of Advanced Computer Science and Applications(IJACSA), 7(4), 2016.
[29] Manjit Kaur, Ahmad Ali AlZubi, Dilbag Singh, Vijay Kumar, Heung-No Lee. "Lightweight Biomedical Image Encryption Approach", IEEE Access, 2023.
[30] Xuanxia Yao, Zhi Chen, Ye Tian, "A lightweight attribute-based encryption scheme for the Internet of Things", Future Generation Computer Systems, Volume 49, Pages 104-112, 2015.
[31] Ren, L., Zhang, D. "A QR code-based user-friendly visual cryptography scheme". Sci Rep 12, 7667 (2022)
[32] V. Petrauskiene and L. Saunoriene, "Application of dynamic visual cryptography for optical control of chaotic oscillations," Vibroengineering PROCEDIA, Vol. 15, pp. 81–87, Dec. 2017.
[33] Paulius Palevicius and Minvydas Ragulskis," Image communication scheme based on dynamic visual cryptography and computer generated holography ",Optics Communications, Volume 335, 2015, Pages 161-167.
[34] Charoghchi, S., Mashhadi, S. "A secure secret image sharing with steganography and authentication by Hamming code (15,11) for compressed images". Multimed Tools Appl 83, 31933–31955 (2024).
[35] Ahmad, S., Abidi, M.R. (2022). "RGB Based Secure Share Creation in Steganography with ECC and DNN". In: Unhelker, B., Pandey, H.M., Raj, G. (eds) Applications of Artificial Intelligence and Machine Learning. Lecture Notes in Electrical Engineering, vol 925. Springer, Singapore.
[36] Salim, A., Sagheer, A.M., Yaseen, L. (2020). "Design and Implementation of a Secure Mobile Banking System Based on Elliptic Curve Integrated Encryption Schema". In: Khalaf, M., Al-Jumeily, D., Lisitsa, A. (eds) Applied Computing to Support Industry: Innovation and Technology. ACRIT 2019. Communications in Computer and Information Science, vol 1174. Springer

Edited by: Anil Kumar Budati
Special issue on: Soft Computing and Artificial Intelligence for wire/wireless Human-Machine Interface
Received: Mar 23, 2024
Accepted: Jun 22, 2024