Privacy Protection for Social Media Based on A Hierarchical Secret Image Sharing Scheme

Sebastien Beugnon, Pauline Puteaux, William Puech

PRIVACY PROTECTION FOR SOCIAL MEDIA BASED ON A HIERARCHICAL SECRET IMAGE SHARING SCHEME

Sébastien Beugnon[⋆†] *Pauline Puteaux*[⋆] *William Puech*[⋆]

[⋆] LIRMM, Univ. Montpellier, CNRS, Montpellier, France
[†]STRATEGIES, Rungis, France

{sebastien.beugnon, pauline.puteaux, william.puech}@lirmm.fr

ABSTRACT

Social network development raises many issues relating to privacy protection for images. In particular, multi-party privacy protection conflicts can take place when an image is published by only one of its owners. Indeed, privacy settings applied to this image are those of its owner and people on the image are not involved in the process. In this paper, we propose a new hierarchical secret image sharing scheme for social networks in order to answer this problem. Based on the disjunctive multi-level approach of Belenkiy applied to images, this solution ensures user privacy, as shown by our obtained experimental results.

***Index Terms*—** Multimedia security, hierarchical secret image sharing, privacy protection, social networks.

1. INTRODUCTION

During the last few decades, multimedia security has become an important issue. With the exponential growth of the Internet, more and more multimedia data – images and videos – are transmitted over the networks and stored on cloud platforms. Social networks are particularly, with more than two billion active users worldwide [1]. Multimedia data passing through these networks are usually personal. Generated in large quantities and mainly by the users themselves, their security is constantly threatened. In particular, privacy protection for everyone when sharing data involving multiple users is a major issue, which can be demonstrated as follows. Alice takes an image with her friends and publishes it on her personal page. Everyone in her social network then has access to this image following the privacy settings she has defined herself. However, her friends, present on the image are not part of the publication procedure. Indeed, they are not consulted and have not given their consent before the publication of the image, which contains information about them [2]. In this context, it is necessary to propose an effective solution to manage these multi-party privacy protection conflicts.

Secret image sharing methods can be used to answer this problem. Inspired by secret sharing schemes developed independently by Blakley [3] and Shamir [4] in 1979, they allow someone to share an image between n users in a secure way [5]. Each user receives information from this process in the form of an image called share. This share is personal, unique and seems visually randomly generated. The original image can be reconstructed if at least k shares among n are gathered together (with $k \leq n$). Indeed, with $k-1$ shares, no information related to the original content can be obtained. The threshold k can be more or less high, depending on the trust level between users in the sharing group.

Multi-level access structure is a generalization of secret sharing and aims to introduce a hierarchy between users. In this kind of scheme, each user is assigned to a level L, associated to a threshold k_L. Note that the lower the level, the more important it is in the hierarchy. Moreover, multi-level access structures can be disjunctive [6, 7] or conjunctive [8]. In particular, in a disjunctive multi-level access structure, a group of users can reconstruct a secret with at least k_L users at level L or at lower levels. Recent secret image sharing schemes integrate hierarchy mechanisms in their approach such as Guo *et al.* [9] inspired by Tassa conjunctive multi-level access structure [8]. Their method uses data hiding to embed shares inside cover images like shadow images. Their work is then extended later by Pakniat *et al.* [10] allowing the lossless reconstruction of the secret and cover images.

In this paper, we propose to use a disjunctive multi-level access structure to share an image that represents several people. First, Alice and her friends define a trust level within their group. Via the social network, they decide to authorize the publication of the image if at least k people among the n present friends in the image give their agreement. When Alice wants to publish an image with her group of friends, they are questioned to know if they accept the disclosure of their faces. If one user agrees, using only their share and the public share, their face can be reconstructed. Moreover, as long as $k' < k$ users accept the reconstruction, only their own faces are revealed. Finally, if k among the n users agree, the whole content of the image is published in the clear domain. Otherwise, the right to privacy is respected and their faces remain protected.

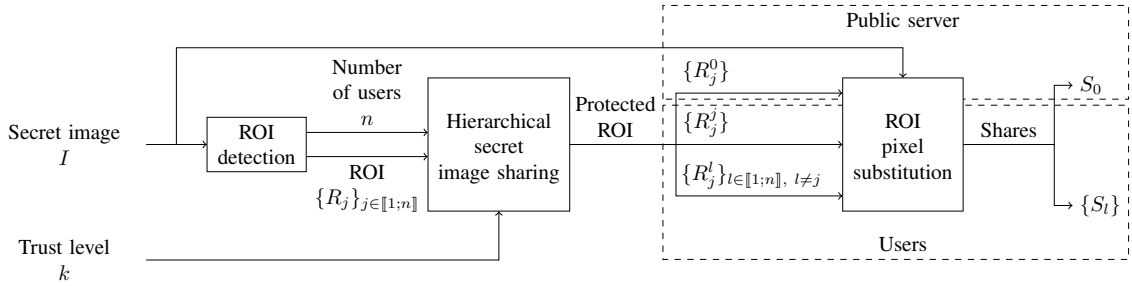

Fig. 1: Overview of the encoding phase.

2. PROPOSED METHOD

The original image is an image which represents a group of n users. Using a face detection algorithm, regions of interest (ROI) R_j, with $j \in [\![1; n]\!]$, associated to each participant are identified on the image. The coordinates of these regions are then used to determine which parts of the image need to be protected by hierarchical secret image sharing. Note that the rest of the image, considered as the background of the image, remains in the clear domain.

To protect the n ROI, we propose to use the disjunctive multi-level secret sharing approach proposed by Belenkiy [7] applied to images. In order to avoid data loss, according to the work of Yang *et al.* [11], we operate the secret sharing scheme in the Galois field $GF(2^8)$. We note x_j with $j \in [\![1; n]\!]$ the value (ID) which is assigned to the j-th participant and the value x_0 refers to the public server:

$$\begin{cases} x_j \in GF(2^8), \\ x_j \neq 0, \\ \forall j, l \in [\![0; n]\!], j \neq l \Leftrightarrow x_j \neq x_l. \end{cases} \tag{1}$$

Moreover, n participants define a trust level within their group. They choose a threshold k such as $1 \leq k \leq n$, that indicates the minimal number of users necessary to reconstruct all the ROI, which means the entire content of the image is in the clear domain. An overview of the encoding phase is provided in Fig. 1.

Each ROI R_j is shared using $n+1$ protected ROI R_j^l, with $l \in [\![0; n]\!]$. Each share S_l, with $l \in [\![0; n]\!]$, has the same size as the original image and the share S_0 is the public share. It is composed of a set of shared pixels (with threshold 2) in the n ROI $\{R_j^0\}_{j\in[\![1;n]\!]}$, and with the original image pixels outside. Other shares $\{S_l\}_{l\neq 0}$, contain the shared pixels (with threshold 2) in the ROI R_j^j associated to the user of ID x_j, the shared pixels (with threshold $k+1$) in other $n-1$ ROI $\{R_j^l\}_{j\in[\![1;n]\!],\ l\neq j}$, and pixels of the background of the original image.

To obtain these shares, each RGB component from each ROI R_j, with $j \in [\![1; n]\!]$, is processed separately. On each component, pixels, encoded in 8 bits, are then sequentially scanned and interpreted as to-be-shared secret values s, such as $s \in GF(2^8)$. To share each secret value s, a random sequence of values $a_0, a_1, \ldots, a_{k-1}$ is generated and a_k is set to s. So, these values are used to define a k-order polynomial:

$$f(x) = \sum_{i=0}^{k} a_i x^i. \tag{2}$$

Using this polynomial, the shared value associated to s from R_j is computed as follows:

- For the public share S_0, the level in the hierarchy is associated to threshold 2 in order to make the reconstruction of R_j possible if the user of ID x_j gives their consent. The shared value is equal to $f^{(k+1-2)}(x_0) = f^{(k-1)}(x_0)$, where $f^{(k-1)}$ is $(k-1)^{\text{th}}$ order derivative of function $f(.)$. Note that this shared value is also used in the reconstruction of R_j, even if the user of ID x_j does not give their consent, but if at least k users are involved in the process.

- For the user of ID x_j, the level in the hierarchy is also associated to threshold 2. Indeed, they have to be able to easily reconstruct their ROI, using only the public share S_0. The shared value is equal to $f^{(k+1-2)}(x_j) = f^{(k-1)}(x_j)$, where $f^{(k-1)}$ is $(k-1)^{\text{th}}$ order derivative of function $f(.)$.

- For users of ID x_l, with $l \neq j$ and $l \neq 0$, the level in the hierarchy is associated to threshold $k+1$. Therefore, each shared value is equal to $f^{(k+1-(k+1))}(x_l) = f(x_l)$. In this case, k participants have to give their consent to allow the full reconstruction of the secret image using the public share and their own shares.

During the decoding phase, there are two possible scenarios, as illustrated in Fig. 2. If the number of users k' is lower than the trust level k, then k' shares $\{S_l\}$, where $l \in [\![1; n]\!]$ and the public share S_0, are used to reconstruct k' ROI $\{R_j\}$ in the clear domain associated to these k' participants. Each secret value s from each R_j can be recovered using a Lagrange interpolation. Indeed, both the user of ID x_j and the public server (of ID x_0) have an equation in terms of two variables a_{k-1} and $a_k = s$. Therefore, by solving the system of

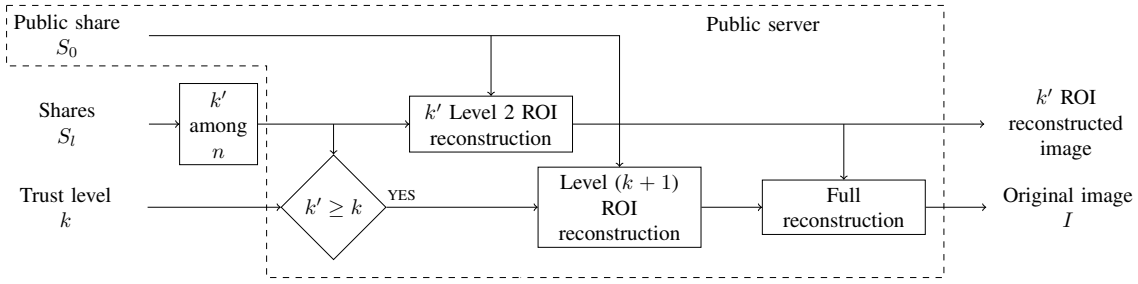

Fig. 2: Overview of the decoding phase.

these two linear equations, they can know the value of s. Note that $n - k'$ ROI of the users who do not participate in the reconstruction remain protected.

If the number of participants k' is equal (or higher) than trust level k, then $n - k'$ ROI associated to the users who do not participate in the reconstruction are also recovered. Indeed, to reconstruct each secret value s, each of $k' \geq k$ participants has an equation in terms of $k+1$ variables $a_0, \ldots, a_k$, where $a_k = s$. Moreover, the public server has an equation in terms of two variables a_{k-1} and $a_k = s$. Thereby, there is a sufficient number of equations to solve the system and learn the value of s_l. After the reconstruction of n ROI $\{R_j\}$, where $j \in [\![1; n]\!]$, the recovered image is exactly the same as the original image. So long as enough users have agreed to the publication of the original image (according to the trust level defined beforehand within the group).

3. EXPERIMENTAL RESULTS

In Fig. 3, we present an example of the whole process of our proposed method with parameters $k = 5$ and $n = 8$. In this case, eight users were identified after detecting the ROI ($n = 8$) and reconstructing the original image is possible when at least five of them give their agreement ($k = 5$). Fig. 3.a illustrates the ROI identified using a face detection algorithm. In the proposed approach, a share S_0 – called public share – is published on social networks, as represented in Fig. 3.b. Moreover, each user of ID x_j, with $j \in [\![1; n]\!]$, receives a personal share S_j where all the ROI are protected. Note that, using this share and the public share S_0 only, each user can reconstruct their own ROI R_j. As an example, Fig. 3.c shows the partially reconstructed image gathering the share S_2 associated to user of ID x_2 and the public share S_0. One can see that the ROI R_2 is available in the clear domain, while all the other ROI remain protected. As long as the number k' of users involved in the reconstruction is lower than the trust level k defined beforehand within the group of users, the original image cannot be entirely reconstructed. For example, as shown in Fig. 3.d, $k' = 3$ shares $S_1,\ S_2$ and S_4 (associated to $x_1,\ x_2$ and x_4) and the public share S_0 are gathered together. As a result, only the background and the ROI $R_1,\ R_2$ and R_4 of users involving in the reconstruction are in the clear domain. For users who do not participate in the reconstruction, the right to privacy is respected and their faces remain protected. Conversely, when at least $k' \geq k$ shares are gathered, for example $k' = 5$ in Fig. 3.e, then the number of users is sufficient to reconstruct the whole content of the original image. k' shares $S_1,\ S_3,\ S_5,\ S_7$ and S_8 associated to the participants of IDs $x_1,\ x_3,\ x_5,\ x_7$ and x_8 are separately gathered with the public share S_0 to reveal the ROI $R_1,\ R_3,\ R_5,\ R_7$ and R_8. Moreover, $n - k' = 3$ remaining ROI $R_2,\ R_4$ and R_6 are reconstructed using the k' shares and the public share together for secret image sharing decoding scheme. Finally, the original image can be entirely and perfectly recovered.

Table 1 resumes the mean results of the following metrics: PSNR (*Peak-Signal-Noise-Ratio*), Shannon's entropy and SSIM (*Structural SIMilarity*) for the generated shares S_l and specifically for each protected ROI R_j^l. When we look at the protected ROI in the shares, we note that the PSNR drops to below 10 dB, the entropy is almost 8 bits per pixel and the SSIM metric falls to almost zero. We can conclude that statistically the ROI are protected inside the shares.

Table 1: Metric results of the images of shares S_l for each protected ROI by the proposed method from Fig. 3.

	PSNR (dB)	SSIM	Entropy (bpp)
I	∞	1.0	7.489
R_1^l	7.463	0.0083	7.925
R_2^l	7.569	0.0070	7.945
R_3^l	8.044	0.0076	7.941
R_4^l	8.029	0.0018	7.935
R_5^l	9.445	0.0104	7.944
R_6^l	7.665	0.0073	7.949
R_7^l	8.380	0.0072	7.943
R_8^l	7.956	0.0078	7.956
Mean	8.069	0.0072	7.942

Fig. 4 illustrates the histograms of all pixel values inside the ROI R_1 in the original image I and inside the associated protected version R_1^0 in the share S_0. We observe that the distribution of pixel values inside the protected ROI R_1^0 is quasi-uniform, meaning that the proposed method is efficient in making the pixel values confidential in each generated share.

Fig. 3: Illustration of the proposed method with parameters $k = 5$, $n = 8$: a) Original image after detecting the ROI associated to the eight users (faces, in red), b) Public share S_0 published on social networks, c) Partially reconstructed image, using the share S_2 associated to user ID x_2 and the public share S_0, d) Partially reconstructed image, after gathering the shares of $k' = 3$ users ($S_1,\ S_2$ and S_4, associated to $x_1,\ x_2$ and x_4) and the public share S_0, e) Entirely and perfectly reconstructed original image, after gathering the shares of at least $k' = 5$ users ($S_1,\ S_3,\ S_5,\ S_7$ and S_8, associated to $x_1,\ x_3,\ x_5,\ x_7$ and x_8) and the public share S_0.

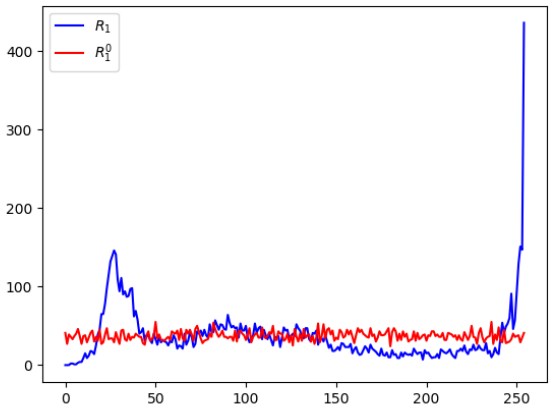

Fig. 4: Histograms of the clear domain ROI R_1 and of one of the associated protected ROI R_1^0.

4. CONCLUSION

In this paper, we proposed an effective way to ensure user privacy on images posted on social networks based on hierarchical secret image sharing. By mutual agreement, n users choose to allow clear visualization of all the regions of interest (ROI) when at least k of them allowed the entire reconstruction. If this threshold is not met, only the ROI associated to users who participate in the reconstruction are revealed, with the help of the public share S_0. The presented experimental results validate the efficiency of our approach in terms of users in real situations and in terms of security. In addition, our method can extend its uses to a more traditional case of multi-party privacy, where all users must give their consent to authorize partial reconstruction. In this case, a threshold (k, k) has to be used during the sharing of the secret image.

5. REFERENCES

[1] "Number of social network users worldwide from 2010 to 2021," https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/, Accessed: 2019-01-14.

[2] J. M. Such and N. Criado, "Multiparty privacy in social media," *Communications of the ACM*, vol. 61, no. 8, pp. 74–81, 2018.

[3] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, 1979, vol. 48, pp. 313–317.

[4] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[5] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[6] G. J. Simmons, "How to (really) share a secret," in *Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology*, 1990, CRYPTO '88, pp. 390–448.

[7] M. Belenkiy, "Disjunctive multi-level secret sharing.," *IACR Cryptology ePrint Archive*, vol. 2008, pp. 18, 2008.

[8] T. Tassa, "Hierarchical threshold secret sharing," *Journal of Cryptology*, vol. 20, no. 2, pp. 237–264, 2007.

[9] C. Guo, C.-C. Chang, and C. Qin, "A hierarchical threshold secret image sharing," *Pattern Recognition Letters*, vol. 33, no. 1, pp. 83–91, 2012.

[10] N. Pakniat, M. Noroozi, and Z. Eslami, "Secret image sharing scheme with hierarchical threshold access structure," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1093–1101, 2014.

[11] C.-N. Yang, P. Li, C.-C. Wu, and S.-R. Cai, "Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach," *Signal Processing: Image Communication*, vol. 31, pp. 1–9, 2015.