01 Jan 2023

Preserving Privacy In Image Database Through Bit-planes Obfuscation

Vishesh K. Tanwar

Ashish Gupta

Sanjay Kumar Madria
Missouri University of Science and Technology, madrias@mst.edu

Sajal K. Das
Missouri University of Science and Technology, sdas@mst.edu

Recommended Citation

V. K. Tanwar et al., "Preserving Privacy In Image Database Through Bit-planes Obfuscation," *Proceedings - 2023 IEEE 39th International Conference on Data Engineering Workshops, ICDEW 2023*, pp. 132 - 137, Institute of Electrical and Electronics Engineers, Jan 2023.
The definitive version is available at https://doi.org/10.1109/ICDEW58674.2023.00027

2023 IEEE 39th International Conference on Data Engineering Workshops (ICDEW) | 979-8-3503-2244-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICDEW58674.2023.00027

Preserving Privacy in Image Database through Bit-planes Obfuscation

Vishesh K. Tanwar, Ashish Gupta, Sanjay Madria, Sajal K. Das

Department of Computer Science, Missouri University of Science and Technology, Rolla, USA
{vktgtd, ashish.gupta, madrias, sdas}@mst.edu

***Abstract*—The recent surge in computer vision applications has caused visual privacy concerns to people who are either users or exposed to an underlying surveillance system. To preserve their privacy, *image obfuscation* lays out a strong road through which the usability of images can also be maintained without revealing any visual private information. However, prior solutions are susceptible to reconstruction attacks or produce non-trainable images even by leveraging the obfuscation ways. This paper proposes a novel bit-planes-based image obfuscation scheme, called Bimof, to protect the visual privacy of the user in the images that are input into a recognition-based system. By incorporating the chaotic system for non-invertible noise with matrix decomposition, Bimof offers strong security and usability for creating a secure image database. In Bimof, it is hard for an adversary to recover the original image, withstanding a malicious server. We conduct experiments on two standard activity recognition datasets, UCF101 and HMDB51, to validate the effectiveness and usability of our scheme. We provide a rigorous quantitative security analysis through pixel frequency attacks and differential analysis to support our findings.**

***Index Terms*—Image obfuscation, Secure image database, Usability, Visual privacy**

I. Introduction

Recently, an unprecedented surge has been seen in the usage of surveillance cameras [1] due to security concerns, causing an explosion of image and video data on cloud servers. Such data are leveraged for identification-related tasks and thus uploaded in *plain form*, which raises privacy concerns to the users as the data may be exploited to gain private visual information either by legitimate image retrieval or by adversaries from database [2]. Consider a scenario of airport surveillance security in which multiple CCTV cameras are deployed to detect suspicious human activities and objects. The recorded images are continuously uploaded to the cloud, inviting adversaries to steal passengers' visual personal identification information (V-PII), such as their face, gender, race, and so on. To protect V-PII, a *privacy assurance* scheme should be integrated with cloud data aggregation services without compromising the utility of the underlying applications.

A naive approach towards preserving V-PII is via obfuscation such as face blurring [3] while uploading on a cloud database. By scaling this idea from face to entire image, prior studies adopted down-sampling [4], [5] and pixelation [6] to conceal V-PII which otherwise is apparent in high-resolution images. Rajput et al. [7] added Gaussian noise into the underlying image before applying down-sampling for obfuscation. Another method, scrambling [8], makes the resultant image visually indiscriminate by disrupting pixels' inter-correlation. A comprehensive survey of image obfuscation techniques is presented in [9]. On a different track, though the cryptography-based approaches such as differential privacy (DP) [10] and fully homomorphic encryption (FHE) [11] can offer strong visual privacy, their effectiveness is limited under machine learning and deep learning algorithms.

Our research is motivated by the following limitations of the current literature. First, though the prior privacy-preserving schemes [8], [11] offer good security by minimizing or breaking the pixels' inter-correlation, the generated obfuscated images *do not contain enough information for training* deep neural networks (DNNs) to achieve adequate accuracy. Second, the blurred [3], down-sampled images [5] have high usability to train highly DNNs, but they are *vulnerable to reconstruction and de-identification attacks*. Third, the obfuscation schemes such as [5] assume that the server is trustworthy because the server designs the underlying obfuscation function for the user, using data-driven DNNs prone to reverse training, thus posing a risk of image reconstruction [12] by the server.

Major Contributions: While addressing the above limitations, we make the following contributions:

- We propose a novel **B**it-planes based **Im**age **O**b**f**uscation scheme, abbreviated as Bimof, to preserve V-PII for creating a secure image database. Unlike the above discussed prior approaches, Bimof offers stronger security against reconstruction and de-identification attacks by injecting non-invertible noise (generated using Lorenz's chaotic system [13]) at a bit-planes level.
- In Bimof, the obfuscation function may not be known to the server, thereby making it independent of the server's intention and robust against adversarial image retrieval from a cloud database.
- By employing two benchmark activity recognition datasets, UCF101 and HMDB51, we evaluate the effectiveness of Bimof through rigorous qualitative and quantitative security analysis and further demonstrate its superiority over the state-of-the-art approaches.

Paper organization: Section II discusses the related work followed by our proposed image obfuscation scheme, Bimof, in Section III. Section IV, we presented the qualitative security analysis using different block sizes and reported the recogni-

2473-3490/23/$31.00 ©2023 IEEE
DOI 10.1109/ICDEW58674.2023.00027

tion accuracies over UCF101 and HMDB51 datasets. Finally, Section V concludes the paper with future directions.

II. Related Work

This section presents the current status of the literature on obfuscation methods. The prior works can be broadly divided into two categories based on the underlying process.

A. Learning-based obfuscation methods

By introducing a privacy-preserving system to access the users' images stored over the online social media database, Ilia et al. [3] focused on blurring the users' faces to prevent leakage of V-PII. In another study [4], a privacy-preserving camera system is presented for patrol robots to detect human faces from extremely low-resolution (eLR) images and then enhance the resolution of the image background (except face pixels) to improve the model accuracy. However, these schemes fail to protect other privacy attributes like gender, race, location, *etc.* Li and Choi [5] proposed an image obfuscation scheme named *DeepBlur* to prevent face re-identification attacks by humans and to invert data-driven DNNs. The authors synthesized the photo-realistic facial image by obfuscating the latent feature space of the unconditional GANs. The qualitative analysis shows the preservation of gender and race when the scheme is evaluated for face datasets. Ryoo et al. [14] introduced a learning-based anonymization scheme to develop an activity recognition system by transforming images into eLR forms. For DNNs training, they aimed to exploit multiple LR videos respective to a single high-resolution (HR) video and embed them with the same representation used for classification.

Ren et al. [15] proposed an adversarial training encoder-decoder-based video anonymizer while maintaining the model's usability. Unlike down-sampling-based approaches, Bai et al. [16] combined HR and eLR videos, utilizing spatial-temporal attention information to improve activity recognition. Purwanto et al. [17] presented a multi-head activity recognition model using self-attention by exploiting the Spatiotemporal information. The authors argue that the model training with super-resolution images and incorporating a teacher-student knowledge distillation approach to eLR images enhances visual privacy. A coupled convolutional neural network using anonymous LR videos and exploiting the optical flow of LR and HR videos is presented in [18] for indoor activity. Recently, in [19], a multi-stream DNN has been proposed for activity recognition on eLR videos, exploiting RGB images and slack mask data. You et al. [20] proposed a reversible privacy-preserving face mosaicing scheme via training an encoder to obtain a protected image and the original facial features. Further, a decoder is used to recover the original face with protected images as input.

B. Non-learning based obfuscation methods

Rajput et al. [7] utilized position-based superpixel transformation and *Gaussian* noise for RGB-depth video database to train a DNN for human activity recognition system over the cloud server. Jeevitha and Prabha [8] proposed a block-based image scrambling technique by decomposing a secret image into multiple discrete wavelet transform planes. Knott et al. [21] developed secure software under a semi-honest threat model to perform common operations in ML frameworks for image classification and speech recognition.

Gilad et al. [11] proposed an FHE scheme for encrypting gray-scale images to train a feed-forward neural network and validated it for the MNIST dataset only. Bost et al. [22] also proposed an FHE-based scheme for naive Bayes, decision trees, and hyperplane decision classifiers. The authors combined FHE without bootstrapping, Quadratic Residuosity, and Paillier cryptosystems [23] for data encryption. Chamikara et al. [10] leveraged the local differential privacy (LDP) to develop a privacy-preserving face recognition protocol to prevent biometric features while authenticating the individual. Wang and Chang [24] proposed a two-party privacy-preserving image classification scheme by perturbating the image information using LDP. They analyzed perturbation's effect satisfying ϵ-LDP on data utility regarding distance and count-based machine learning algorithms. Chen et al. [25] presented a secure multi-classification scheme to address the privacy leakage in robot systems using DNN. The authors used homomorphic encryption for secure calculation protocols to adopt two activation and cost function pairs.

Contrasting existing work that protects pre-defined visual attributes like faces and gender, our proposed scheme performs obfuscation over the image to protect the complete image, not some specific privacy attributes. However, our extended version will contain privacy experiments showing the preservation of specific attributes.

III. Proposed Obfuscation scheme

In this section, we propose an image obfuscation scheme, Bimof, to conceal users' V-PII when the data are stored on the cloud database. Unlike prior schemes [26], [27] that obfuscate images by pixel permutation, Bimof follows a novel idea in which each pixel of the input image is obfuscated without altering its location. Specifically, we add randomness and non-invertible noise to each pixel intensity value while preserving useful features for DNN model training. Bimof produces *non-invertible* image, i.e., the original image cannot be reconstructed from its obfuscated form, thereby protecting it from gradient reconstruction, model inversion, and de-identification attacks.

A. Random noise generation

As Bimof aims to insert a non-invertible noise into the input image, we reviewed the related literature. We found that chaotic structures [13] are a favorable choice for securing image information as they are unpredictable, non-reproducible, and intrinsically coherent. Following [13], we utilize Lorenz's chaotic structures on three variables x, y, z, defined as

$$\frac{dx}{dt} = \alpha(y - x), \quad \frac{dy}{dt} = \beta x - y - xz, \frac{dz}{dt} = xy - \gamma z \quad (1)$$

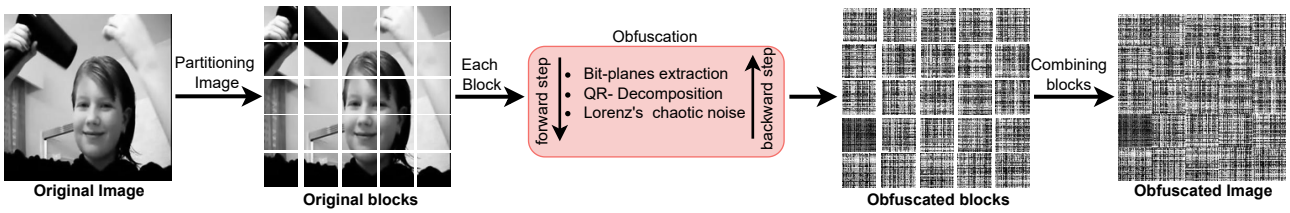


Fig. 1: The proposed image obfuscation scheme (Bimof).

where α, β, γ are the system parameters. Solution hyperplane of the system 1 has chaotic nature for $(\alpha = 10, \beta = 28, \gamma = 8/3)$ [13]. Let $\mathcal{S} \in \mathbb{R}^{num_{sol} \times 3}$ denote a solution matrix for system 1, where num_{sol} is total number of solutions. Bimof leverages these vectors to perturbating the QR components of a bit-plane in Section III-B.

B. Bimof Scheme

Bimof obfuscates the input image through *block-based bit-planes obfuscation*. Fig. 1 demonstrates the overall obfuscation process of our scheme. For a given input gray-scale image I, Bimof divides it into blocks, incorporates the non-invertible DP noise mechanism to each block, and then performs reconstruction to obtain the obfuscated image I_{obs}. Intuitively, the assimilated noise would spread and accumulate to each pixel intensity value during reconstruction while keeping its location unaltered in the obfuscated image I_{obs}.

Let the dimension of I is $m \times n$ which we partition into L non-overlapping blocks, each of dimension $\tau_1 \times \tau_2$, denoted as $\left\{I_b^1, I_b^2, \cdots I_b^L\right\}$, where $L = \frac{m \times n}{\tau_1 \times \tau_2}$ is a positive integer. Each block may be perceived as a gray-scale image of dimension $\tau_1 \times \tau_2$. Utilizing the property that a gray-scale image can be decomposed exactly into eight bit-planes, our obfuscation scheme for each of the L blocks is as follows.

Forward step: For l^{th} gray-scale block I_b^l, Bimof first partitions it into eight bit-planes, which are denoted as $\mathcal{BP}_1^l, \mathcal{BP}_2^l, \cdots, \mathcal{BP}_8^l$, $1 \leq l \leq L$, where $\mathcal{BP}_k^l$ contains only binary values obtained via decimal to binary conversion, defined as

$$\mathcal{BP}_k^l = \left\lfloor \frac{[I_b^l]}{2^{k-1}} \right\rfloor \ mod\ 2 \quad \forall \quad k = 1, 2, .., 8 \tag{2}$$

where $\lfloor \cdot \rfloor$ represents the floor function.

It is well established in the literature that the first four least-significant bit-planes contain nearly $6\% - 7\%$, and the last four most significant bit-planes carry $93\% - 94\%$ of total image information (For the information percentage, please refer the Table 1 in [28]). Mathematically, the percentage of information that an i^{th} bit-plane contains is

$$P(i) = \frac{2^i}{\sum_{j=0}^{7} 2^j} \qquad \forall \qquad i = 0, 1, .., 7 \tag{3}$$

Now, we compute *QR-decomposition* of k^{th} bit-plane of I_b^l as

$$\mathcal{BP}_k^l = \left[\mathcal{BP}_k^l\right]^Q \times \left[\mathcal{BP}_k^l\right]^R, \tag{4}$$

where $\left[\mathcal{BP}_k^l\right]^Q$ and $\left[\mathcal{BP}_k^l\right]^R$ are *orthogonal* and *upper-triangular* feature maps of dimensions $\tau_1 \times \tau_2$. The QR-decomposition technique is empathetic with small perturbation, i.e., a small perturbation in QR components makes a significant variance in the original bit-plane upon reconstruction, thereby introducing the desired level of randomness in the generated obfuscated image during reconstruction [29]. By considering a bit-plane of size 3×3, Fig. 2 illustrates the perturbation in the bit-plane values by altering the QR components of the original bit-plane. Here, Bimof leverages the vectors $[n_1^1, n_1^2]$ and $[n_2^1, n_2^2]$, generated by Lorenz's chaotic structures in Section III-A, to produce an non-invertible noise for pixel location (i, j) as

$$\begin{aligned} noise_{ij}^Q &= n_1^1 + (n_2^1 - n_1^1) \times rand_{ij}^Q \\ noise_{ij}^R &= n_2^1 + (n_2^2 - n_1^2) \times rand_{ij}^R, \end{aligned} \tag{5}$$

where $rand_{ij}^Q$ and $rand_{ij}^R$ are differentially private values obtained over Gaussian distribution $\mathcal{N}(0, 1)$, $1 \leq i \leq \tau_1$ and $1 \leq j \leq \tau_2$. Now, we obfuscate each of the QR components of the bit-plane $\mathcal{BP}_k^l$ by

$$\begin{aligned} \left[\mathcal{BP}_k^l\right]_{obs}^Q (i, j) &= \left[\mathcal{BP}_k^l\right]^Q (i, j) + noise_{ij}^Q \\ \left[\mathcal{BP}_k^l\right]_{obs}^R (i, j) &= \left[\mathcal{BP}_k^l\right]^R (i, j) + noise_{ij}^R. \end{aligned} \tag{6}$$

It is important to note that independent randomness is injected at every pixel. In addition, as $noise_{ij}^Q$ and $noise_{ij}^R$ incorporate the chaotic noise vectors and DP Gaussian mechanism, projecting the planes Q and R planes over the random and non-invertible obfuscated planes, $\left[\mathcal{BP}_k^l\right]_{obs}^Q$ and $\left[\mathcal{BP}_k^l\right]_{obs}^R$.

Backward step: We perform inverse QR-decomposition, using Eq. 4, followed by normalization and thresholding to obtain obfuscated bit-planes. Since the results of inverse QR-decomposition contains non-binary real values, Bimof performs normalization over the range $[0, 1]$ and then applies binary thresholding at the mean value of the normalized form, which in turn generates the obfuscated bit-plane $\left[\mathcal{BP}_k^l\right]_{obs}$. It is important to note that the normalization and thresholding make our scheme a non-invertible obfuscation scheme protecting users' V-PII from malicious reconstruction and de-identification attacks from the image database. Later, we construct the obfuscated block by

$$[I_b^l]_{obs} = \sum_{k=1}^{8} [\mathcal{BP}_k^l]_{obs} \times 2^{k-1}, \quad 1 \leq l \leq L \tag{7}$$

After performing obfuscation over all L blocks, we concatenate all the obfuscated blocks $\left\{\left[I_b^1\right], \left[I_b^2\right], ... \left[I_b^L\right]\right\}$ at the

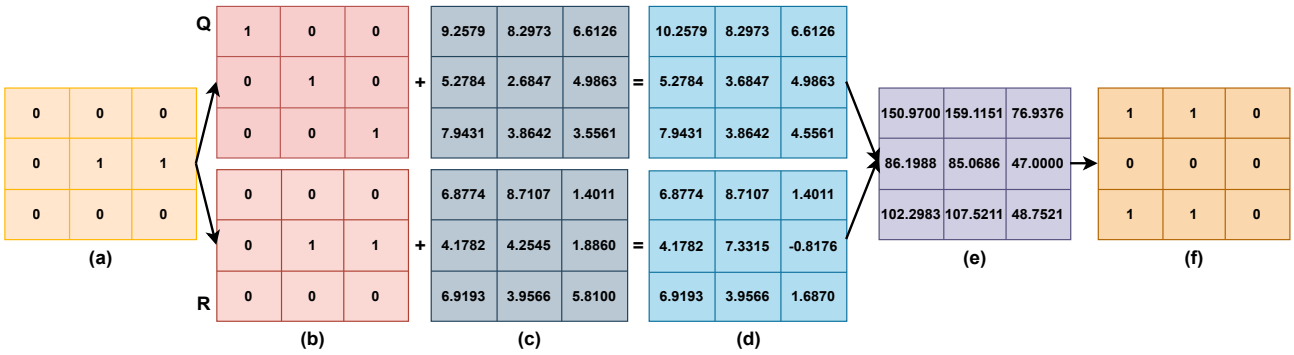


Fig. 2: Intermediate outputs of bit-plane obfuscation. (a) Original bit-plane, (b) QR-components, (c) Noise matrices as defined in Eq. 5, (d) Noisy QR components (Eq. 6), (e) Resultant of inverse QR-decomposition, and (f) Obfuscated bit-plane obtained by normalizing and thresholding (e).

corresponding locations of $\{I_b, {}^1I_b, {}^2I_b ... {}^LI_b\}$ to obtain our final obfuscated image I_{obs}. We independently perform Bimof to all color channels for an RGB-color image.

IV. Experiments and Results Discussion

We validate the effectiveness of the proposed scheme over the activity recognition system using benchmark video datasets, namely *HMDB51* [30] and *UCF101* [31]. This section reports and critically analyses the results obtained after conducting an extensive set of experiments.

A. Dataset Description

1) **HMDB51** dataset [30] consists of 6849 realistic video clips with 51 classes of human activities, and there exist more than 100 clips for each category; some of the activities are "throw", "pull-ups," "pick," , *etc.*
2) **UCF101** [31] is also a standard dataset for evaluating HAR systems. It consists of 13320 video clips divided into 101 classes, like "blow dry hair", "push-ups," , *etc.*

Experimental setting: We implemented the proposed scheme in *Python* language on Ubuntu 20.14 64-bit, over HP workstation with Nvidia Quadro P5000 graphic card and Intel Xeon(R) 5120 CPU @2.20×56 GHz. Four state-of-the-art DCNNs, namely *ResNet18*, *ResNet34*, *ResNet50*, and *VGG16* are employed for activity recognition system. Training hyperparameters: batch size $= 128$, epochs $= 125$, optimizer $= adam$, learning rate $= 1e^{-3}$, cosine annealing lr-scheduler, and negative log-likelihood loss. While maintaining the original ratio of the train-test split, we use 10% of training data for validation. The size of each block is a factor of 200×200 (the dimension of the original frame).

B. Impact of the block size

As mentioned in our scheme, the input image is divided into non-overlapping blocks of dimension $\tau_1 \times \tau_2$. Here, we visually show the obfuscated images obtained with varying block sizes: 5×5, 10×10, 20×20, 25×25, and 40×40, for the original image of *hair blowing* activity of dimension 200×200 in Fig. 3. The level of randomness in an obfuscated image is proportional to the chosen block size. For instance, an obfuscated image using block size 5×5 reveals a few edges, activity attributes, and object(s) location, whereas an

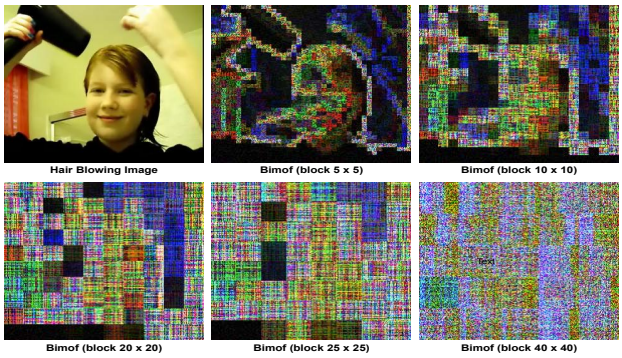
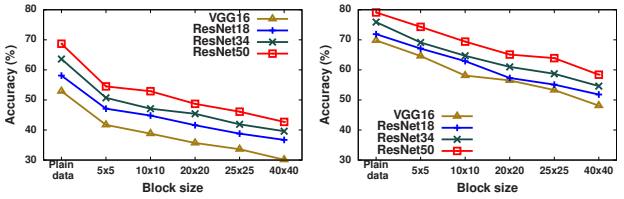


Fig. 3: Comparison of Bimof obfuscated images with varying block size. A larger block size offers better privacy.

obfuscated image with block size 40×40 conceals such information. It is worth mentioning that an adversary cannot extract sensitive information from the obfuscated images (stored in the image database in the cloud) for large block sizes; however, it comes at the cost of degraded accuracy, which we validated empirically, and the results are reported in the next section.

C. Recognition accuracy analysis

At first, we conducted experiments to evaluate the recognition accuracy of the considered models in the plain and obfuscated data domain, and the obtained results are reported in Fig. 4. Our obfuscation scheme is model-agnostic, meaning it works with different models without requiring any change in the underlying process/steps, addressing the *Model architecture dependency* limitation of the existing scheme. Moving ahead with the results, all the models lose the accuracy by an admissible magnitude (approximately $15\% - 18\%$) on obfuscated data compared to the ones with plain data. The magnitude of the difference depends on the chosen block size during obfuscation. For instance, the best-performing model *ResNet50* shows an accuracy drop of $\sim 11.8\%$ from plain data to least obfuscation block 5×5 and 14% from block 5×5 to 40×40, for HMDB51 dataset. The reason for such a drop is elevated perturbations in spatial information with larger block size, breaking the inter-correlation among the neighboring pixels and eventually affecting the models' learning, which solves the limitation of *security and usability*. Still, it paid off in terms of stronger protection of visual information. Thus, our



(a) Using HMDB51 dataset (b) Using UCF101 dataset

Fig. 4: Recognition accuracy (%) on plain data and obfuscated data with varying block sizes.

proposed scheme enables the users to choose an appropriate block size based on how strong the protection of personal information they desire is, which finally addresses the final limitation of the need for *trusted server*.

D. Security analysis

This section presents the security analysis of the proposed obfuscation scheme and various standard cryptographic attacks practiced by an adversary to extract V-PII from an obfuscated image to de-identify an individual's identity. The extended version of this work will explain the theoretical and information-based mathematical theorems and proofs.

1) ***Pixel-frequency based attack****:* In this attack, an adversary computes the frequency of each pixel intensities of the obfuscated image (I_{obs}) and attempts to extract meaningful information from the original image (I). Though it seems a trivial attack, the adversary may learn quite a bit of the original image if an underlying obfuscation scheme does not disrupt such frequencies. Ideally, the frequencies of I_{obs}'s pixels must be uniform and unrelated to I. Figure 5 depicts channel-wise pixel-frequencies for (a) *hair blowing plain image* (shown in Figure 3), (b) encryption [32], (c) noise obfuscation [7], and (d) proposed scheme using 40×40 block. In [32], a bit-plane-based chaotic image encryption scheme is proposed with large key space using the SHA-512 Hash function and dynamic cryptographic properties. We observe that encryption offers more uniform (almost ideal) pixel frequencies than the proposed one. Still, the model might not be able to learn over encrypted images, resulting in bad accuracy. In contrast, our scheme has uniform frequencies after obfuscation while securing a usable accuracy.

2) ***Information entropy****:* Entropy quantifies the amount of randomness present in the data. Higher entropy is desirable to conceal private visual information of an obfuscation image. For an N-bit image I_{obs} with T distinct pixel intensities, the entropy would stay in range $[0, N]$, and computed as $-\sum_{t=0}^{T-1} p(t)\, log_2(p(t))$. We compute entropy over the ten randomly chosen images from both the datasets, including the one shown in Fig. 3 and report the average channel-wise results in Table I, which clearly shows the effectiveness of our scheme by defeating all the existing ones, particularly with large block sizes. With block 40×40, the mean entropy is 7.93, close to a maximum possible value of 8.

3) ***Differential analysis****:* Through differential analysis, we examine the change in two different obfuscated forms of a plain image $I \in \mathbb{R}^{M \times N}$ with small perturbations. Specifically,

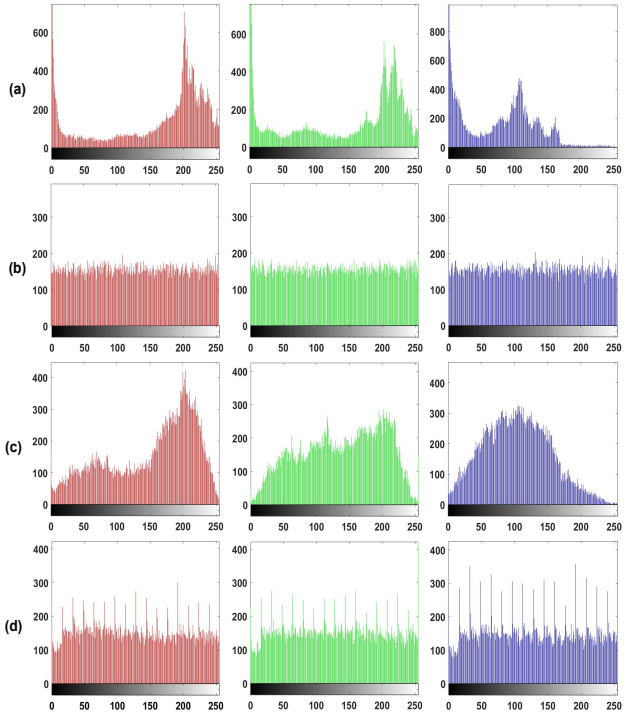


Fig. 5: Channel-wise pixel-frequencies for (a) original image, (b) encryption scheme [32], (c) noise obfuscation scheme [7], and (d) proposed scheme with block size 40×40. x-axis and y-axis indicate the pixel intensity values in $[0, 255]$ and their frequencies, respectively.

we perturb I with a pixel intensity value and obtain obfuscated forms before and after perturbation, say I_{obs_1} and I_{obs_2}, and then compute their difference percentage ($\mathcal{DP}$), defined as

$$\mathcal{DP} = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N} \mathcal{D}(m,n)}{M \times N} \times 100,$$

$$\text{where} \quad \mathcal{D}(m,n) = \begin{cases} 0, & \text{if } I_{obs_2}(m,n) = I_{obs_1}(m,n) \\ 1, & \text{if } I_{obs_2}(m,n) \neq I_{obs_1}(m,n). \end{cases}$$

In Table II, we present the channel-wise scores averaged over ten randomly chosen images from both datasets. The obtained mean (over channels) $\mathcal{DP}$ lies in the range 87%-98% (higher is better), signifying sufficient variations in the pixel intensities of two obfuscated images I_{obs_1} and I_{obs_2}. Our scheme achieved better scores with block sizes 20×20 and above. In contrast, our scheme significantly improves the DP over noise obfuscation [7], and encryption [32] algorithms.

TABLE I: Entropy results for different obfuscation schemes.

	Red	Green	Blue	Mean	Use	Sec
Original	7.25	7.28	6.84	7.13	✓	×
Encryption [32]	7.73	7.77	7.43	7.64	×	✓
Noise obfuscation [7]	7.47	7.47	7.43	7.64	×	✓
Bimof (block 5×5**)**	7.01	6.96	6.77	6.91	✓	✓
Bimof (block 10×10**)**	7.50	7.52	7.36	7.46	✓	✓
Bimof (block 20×20**)**	7.83	7.85	7.79	7.82	✓	✓
Bimof (block 25×25**)**	7.91	7.91	7.82	7.88	✓	✓
Bimof (block 40×40**)**	**7.93**	**7.93**	**7.86**	**7.91**	✓	✓

Use: Usability and Sec: Security.

TABLE II: $\mathcal{DP}$ for different obfuscation schemes.

	Red	Green	Blue	Mean
Encryption [32]	99.63%	99.66%	99.62%	99.64%
Noise obfuscation [7]	93.98%	92.94%	92.54%	93.15%
Bimof (block 5×5)	86.83%	87.04%	86.38%	86.75%
Bimof (block 10×10)	91.69%	91.70%	91.34%	91.58%
Bimof (block 20×20)	96.38%	96.10%	96.03%	96.17%
Bimof (block 25×25)	97.25%	97.77%	96.91%	97.31%
Bimof (block 40×40)	98.23%	98.08%	97.73%	98.01%

V. Conclusion

We proposed a bit-planes-based scheme, Bimof, for protecting the individual's private visual information in the images uploaded on the cloud to store. By incorporating Lorenz's chaotic noise over bit-planes followed by QR-decomposition, we made our scheme robust against the reconstruction attacks while preserving enough information in the obfuscated data for model training. Through extensive experiments on UCF101 and HMDB51 datasets, Bimof is evaluated qualitatively and quantitatively with rigorous analysis of security and usability (accuracy). Experimental results demonstrated that Bimof reveals almost zero V-PII by breaking pixel correlation, disrupting pixel frequency, and adding randomness while significantly outperforming the prior schemes on accuracy. We also observed a trade-off between the recognition accuracy and security level with varying block sizes, enabling users to choose the appropriate size based on the underlying application. In the future, we will exploit the correlation between the original image and its obfuscated version to gain recognition accuracy along with information-theoretic security analysis.

References

[1] O. Elharrouss, N. Almaadeed, S. Al-Maadeed, A. Bouridane, and A. Beghdadi, "A combined multiple action recognition and summarization for surveillance video sequences," *Applied Intelligence*, vol. 51, no. 2, pp. 690–712, 2021.

[2] S. Guo, J. Xu, C. Zhang, C. Xu, and T. Xiang, "Imageproof: Enabling authentication for large-scale image retrieval," in *2019 IEEE 35th International Conference on Data Engineering (ICDE)*. IEEE, 2019, pp. 1070–1081.

[3] P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks," in *Proceedings of the 22nd ACM SIGSAC Conference on computer and communications security*, 2015, pp. 781–792.

[4] M. U. Kim, H. Lee, H. J. Yang, and M. S. Ryoo, "Privacy-preserving robot vision with anonymized faces by extreme low resolution," in *International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2019, pp. 462–467.

[5] T. Li and M. S. Choi, "Deepblur: A simple and effective method for natural image obfuscation," *arXiv arXiv:2104.02655*, vol. 1, 2021.

[6] L. Fan, "Image pixelization with differential privacy," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2018, pp. 148–162.

[7] A. S. Rajput, B. Raman, and J. Imran, "Privacy-preserving human action recognition as a remote cloud service using rgb-d sensors and deep cnn," *Expert Systems with Applications*, vol. 152, p. 113349, 2020.

[8] S. Jeevitha and N. Amutha Prabha, "Novel medical image encryption using dwt block-based scrambling and edge maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3373–3388, 2021.

[9] J. R. Padilla-López, A. A. Chaaraoui, and F. Flórez-Revuelta, "Visual privacy protection methods: A survey," *Expert Systems with Applications*, vol. 42, no. 9, pp. 4177–4195, 2015.

[10] M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, "Privacy preserving face recognition utilizing differential privacy," *Computers & Security*, vol. 97, p. 101951, 2020.

[11] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy," in *Proceedings of the International Conference on Machine Learning*, 2016, pp. 201–210.

[12] J. Jeon, j. Kim, K. Lee, S. Oh, and J. Ok, "Gradient inversion with generative image prior," in *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 34, 2021, pp. 29 898–29 908.

[13] I. S. Badr, A. G. Radwan, E.-S. M. El-Rabaie, L. A. Said, G. M. El Banby, W. El-Shafai, and F. E. Abd El-Samie, "Cancellable face recognition based on fractional-order lorenz chaotic system and haar wavelet fusion," *Digital Signal Processing*, vol. 116, p. 103103, 2021.

[14] M. Ryoo, K. Kim, and H. Yang, "Extreme low resolution activity recognition with multi-siamese embedding learning," in *Proceedings of the Conference on Artificial Intelligence (AAAI)*, vol. 32, no. 1, 2018.

[15] Z. Ren, Y. J. Lee, and M. S. Ryoo, "Learning to anonymize faces for privacy preserving action detection," in *Proceedings of the European Conference on Computer Vision (ECCV)*, 2018, pp. 620–636.

[16] Y. Bai, Q. Zou, X. Chen, L. Li, Z. Ding, and L. Chen, "Extreme low resolution activity recognition with confident spatial-temporal attention transfer," *arXiv preprint arXiv:1909.03580*, 2019.

[17] D. Purwanto, R. Renanda Adhi Pramono, Y.-T. Chen, and W.-H. Fang, "Extreme low resolution action recognition with spatial-temporal multi-head self-attention and knowledge distillation," in *Proceedings of the IEEE International Conference on Computer Vision Workshops (ICCVw)*, 2019, pp. 961–969.

[18] J. Liu and L. Zhang, "Indoor privacy-preserving action recognition via partially coupled convolutional neural network," in *2020 International Conference on Artificial Intelligence and Computer Engineering (ICAICE)*. IEEE, 2020, pp. 292–295.

[19] P. Russo, S. Ticca, E. Alati, and F. Pirri, "Learning to see through a few pixels: Multi streams network for extreme low-resolution action recognition," *IEEE Access*, vol. 9, pp. 12 019–12 026, 2021.

[20] Z. You, S. Li, Z. Qian, and X. Zhang, "Reversible privacy-preserving recognition," in *2021 IEEE International Conference on Multimedia and Expo (ICME)*. IEEE, 2021, pp. 1–6.

[21] B. Knott, S. Venkataraman, A. Hannun, S. Sengupta, M. Ibrahim, and L. van der Maaten, "Crypten: Secure multi-party computation meets machine learning," *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 34, pp. 4961–4973, 2021.

[22] R. Bost, R. A. Popa, S. Tu, and S. Goldwasser, "Machine learning classification over encrypted data." in *NDSS*, 2015.

[23] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.

[24] S. Wang and J. M. Chang, "Privacy-preserving image classification in the local setting," *arXiv preprint arXiv:2002.03261*, 2020.

[25] Y. Chen, Y. Ping, Z. Zhang, B. Wang, and S. He, "Privacy-preserving image multi-classification deep learning model in robot system of industrial iot," *Neural Computing and Applications*, pp. 1–18, 2020.

[26] P. Li, J. Xu, J. Mou, and F. Yang, "Fractional-order 4d hyperchaotic memristive system and application in color image encryption," *EURASIP Journal on Image and Video Processing*, vol. 2019, no. 1, p. 22, 2019.

[27] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the lss chaotic map and single s-box," *IEEE Access*, vol. 8, pp. 25 664–25 678, 2020.

[28] Z.-l. Zhu, W. Zhang, K.-w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

[29] P. Rakheja, R. Vig, and P. Singh, "Double image encryption using 3d lorenz chaotic system, 2d non-separable linear canonical transform and qr decomposition," *Optical and quantum electronics*, vol. 52, no. 2, pp. 1–21, 2020.

[30] H. Kuehne, H. Jhuang, E. Garrote, T. Poggio, and T. Serre, "Hmdb: a large video database for human motion recognition," in *Proceedings of the International Conference on Computer Vision (ICCV)*. IEEE, 2011, pp. 2556–2563.

[31] K. Soomro, A. R. Zamir, and M. Shah, "Ucf101: A dataset of 101 human actions classes from videos in the wild," *arXiv preprint arXiv:1212.0402*, 2012.

[32] W. Zhou, X. Wang, M. Wang, and D. Li, "A new combination chaotic system and its application in a new bit-level image encryption scheme," *Optics and Lasers in Engineering*, vol. 149, p. 106782, 2022.