Compressione Dati - AA 2018/2019

IMAGE SCRAMBLING

Grayscale-Based block scrambling image encryption for social networking services

Warit Sirichotedumrong, Tatsuya Chuman, Shoko Imaizumi and Hitoshi Kiya

Prof. Bruno Carpentieri

Angelo Settembre
Pasquale Settembre

Introduzione

- La rapida crescita di Internet e sistemi multimediali ha causato l'incremento di utilizzo di immagini e video particolarmente sui Social Networks.
- Tuttavia, questa enorme condivisione multimediale ha sollevato serie preoccupazioni riguardanti la ***privacy***.

Privacy

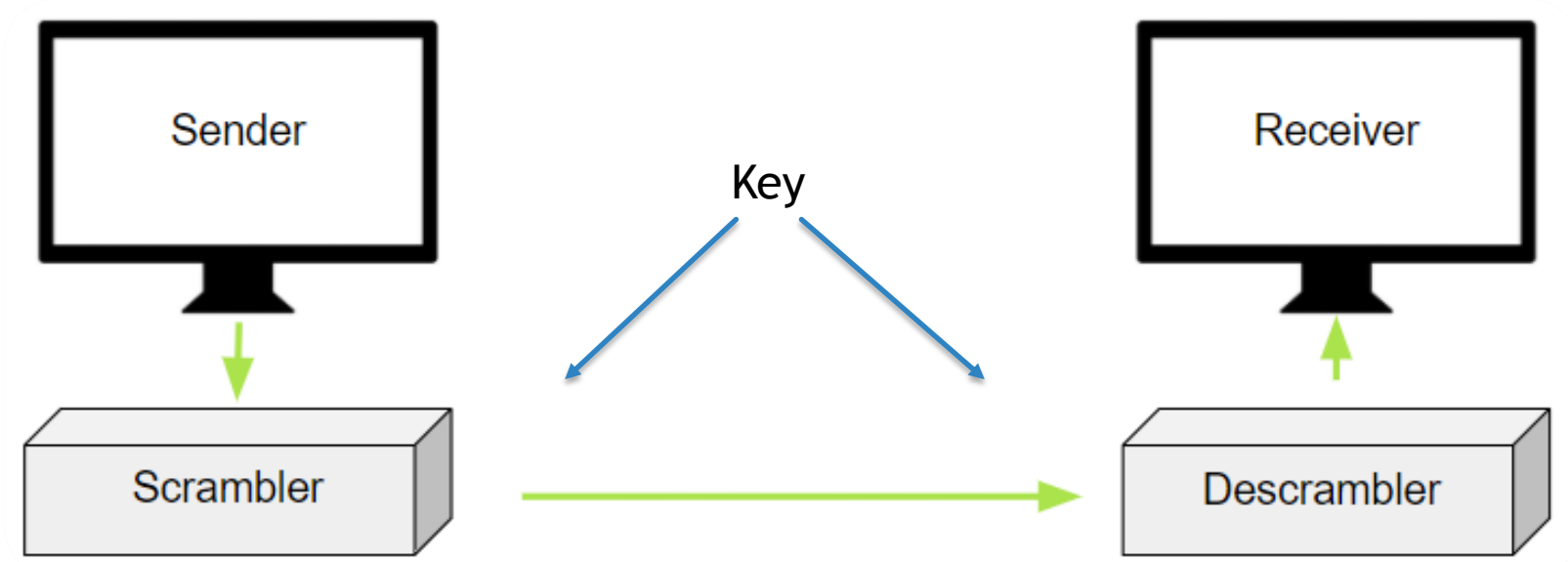
- Le foto possono essere viste da chiunque
- Combinando più foto è possibile identificare una persona
- Leak di foto private sui social network come Facebook, Twitter, etc
  - Social Networking Service (SNS)

Stato dell'arte

- Effettuare una completa cifratura dell'immagine utilizzando noti crittosistemi come RSA o AES
  - SVANTAGGI
    - Costo per la cifratura
    - Incompatibilità con il formato per l'utilizzo in molte applicazioni

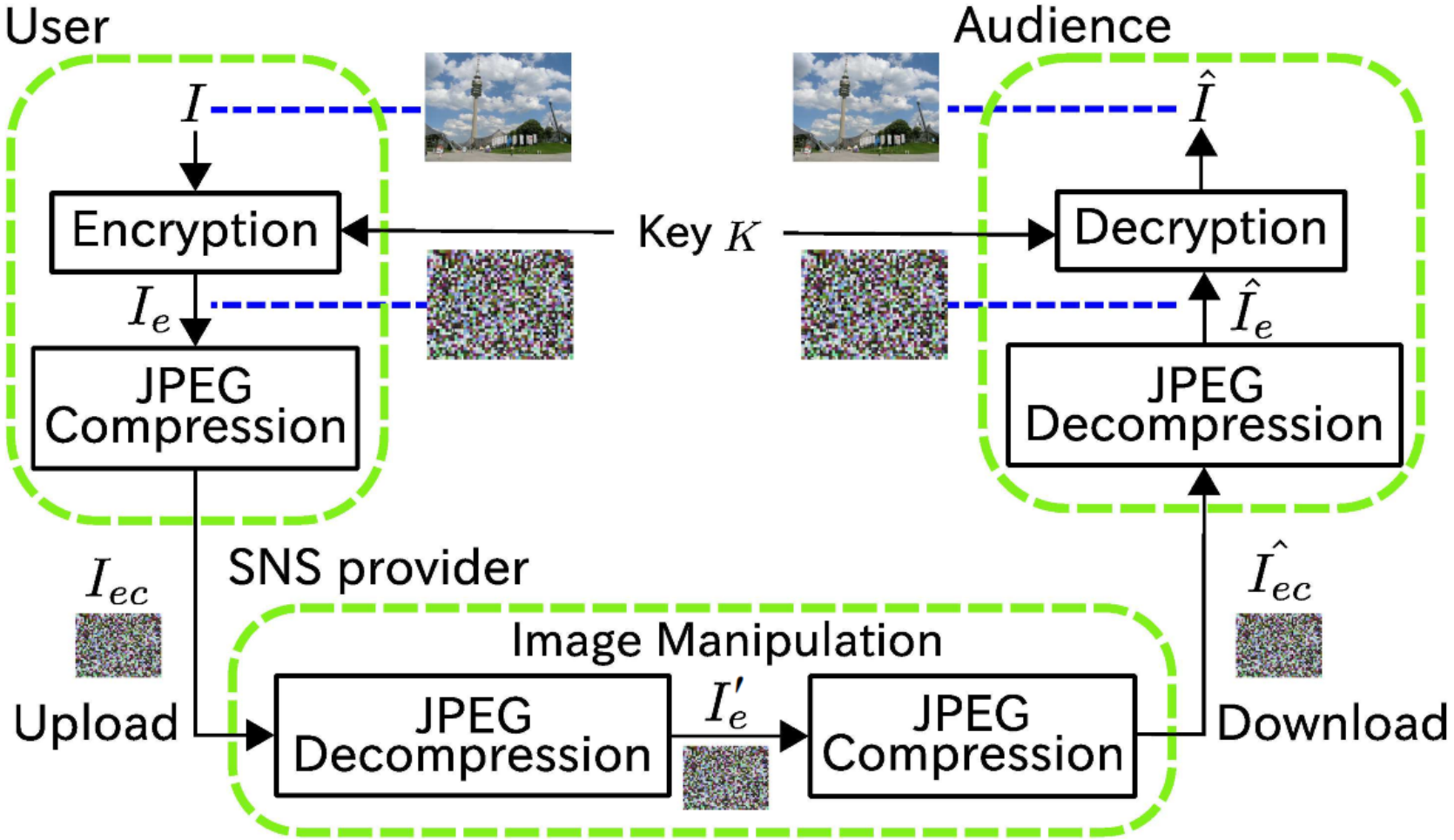
Scrambling

- Permette la trasmissione e la ricezione dei dati in modo digitale e criptato
- Prima di inviare i dati, lo **scrambler** ne manipola il flusso
- Una volta arrivati a destinazione, il **descrambler** li riporta nel formato originario



Encryption-then-Compression (EtC)

Encryption-then-Compression method for SNS



SNS image manipulation

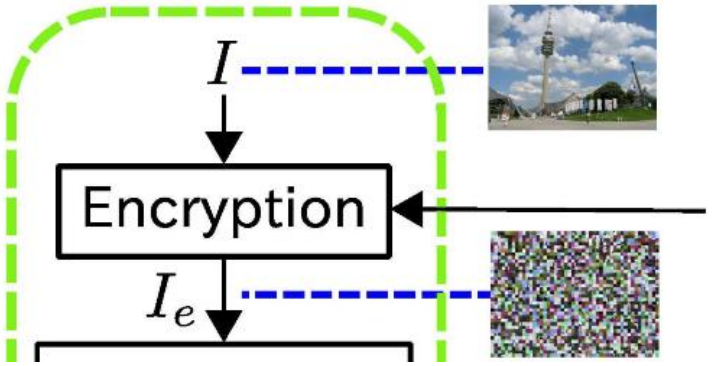
- La maggior parte dei SNS provider manipolano le immagini caricate dagli utenti
  - *Rescaling* della risoluzione e *ricompressione* con parametri differenti per diminuire la dimensione delle immagini
- La qualità delle immagini ricompresse dai provider SNS è ridotta

SNS image manipulation - 1

SNS provider	Uploaded JPEG file		Downloaded JPEG file	
	Sub-sampling ratio	Q_f	Sub-sampling ratio	Q_f
Twitter (Up to 4096×4096 pixels)	4:4:4	low	No recompression	
		high	4:2:0	85
	4:2:0	1,2,...84	No recompression	
		85,86,...100	4:2:0	85
Facebook (HQ, Up to 2048×2048 pixels)	4:4:4	1,2,...100	4:2:0	71,72,...85
Facebook (LQ, Up to 960×960 pixels)	4:2:0			

- Lo standard più utilizzato dai SNS provider per la compressione di immagini è lo standard **JPEG**
- **Twitter**
  - effettua ricompressione dell'immagine caricata se il quality factor $Q_f > 84$
  - Altrimenti, l'immagine non viene ricompressa
- **Facebook**
  - effettua sempre ricompressione dell'immagine

Block scrambling-based image encryption scheme



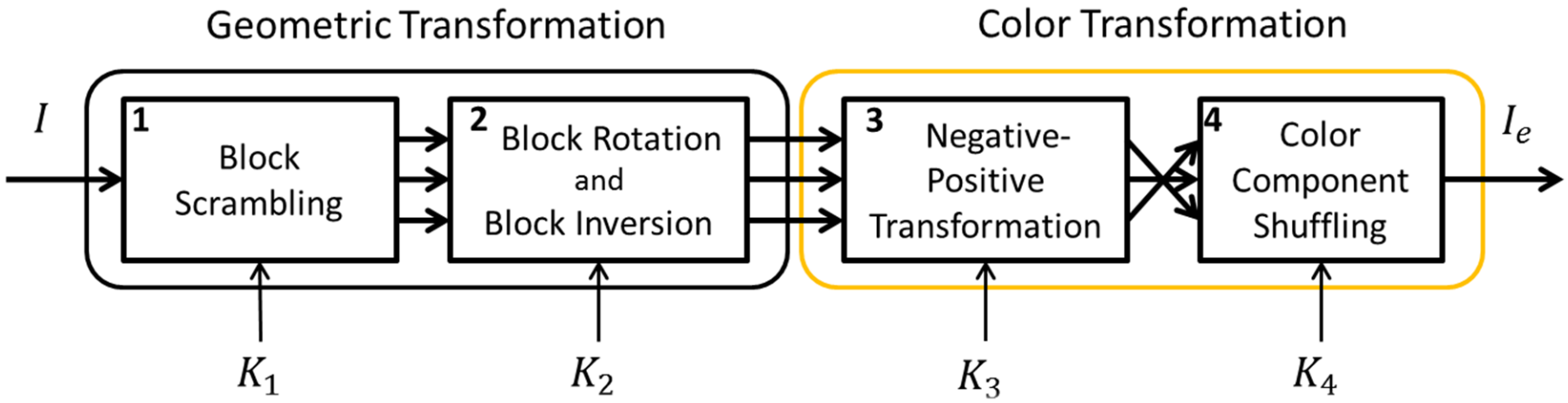
Block scrambling-based image encryption scheme

- Una immagine (I) con $M \times N$ pixel è divisa in blocchi non sovrapposti, ciascuno di $B_x \times B_y$ pixel
- Il numero di blocchi divisi, n, è rappresentato da:

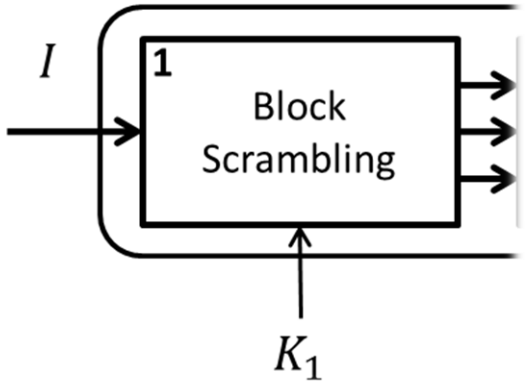
$$n = \lfloor \frac{M}{B_x} \rfloor \times \lfloor \frac{N}{B_y} \rfloor$$

Block scrambling-based steps

- Per la generazione di una immagine cifrata (I_e), ogni blocco diviso viene elaborato usando 4 passi

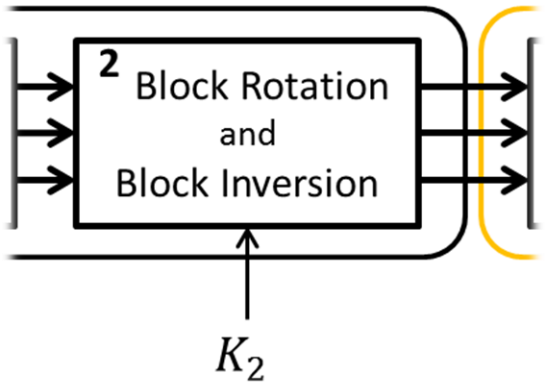


Step - 1



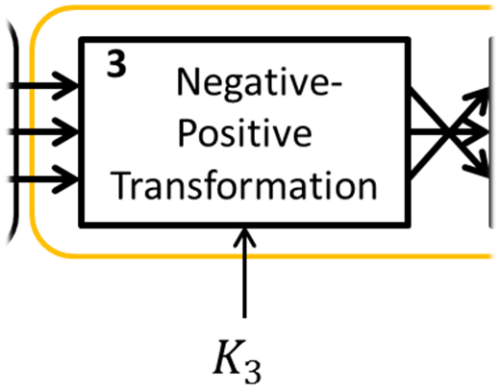
Step1: Divide an image with $M \times N$ pixels (I) into blocks with $B_x \times B_y$ pixels, and permute the divided blocks randomly based on the random integer which is generated by a secret key K_1.

Step - 2



Step2: Randomize the integer using a secret key K_2, then rotate and invert each block according to the previously randomized integer.

Step - 3

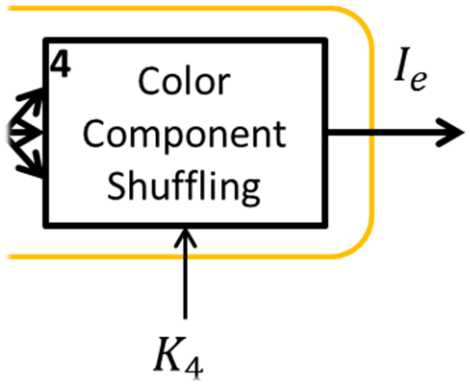


Step3: Apply the negative-positive transformation to each block using a random binary integer generated by a secret key K_3. A transformed pixel of ith block is represented by p' and computed as

$$p' = \begin{cases} p & (r(i) = 0) \\ p \oplus (2^L - 1) & (r(i) = 1) \end{cases} \quad (2)$$

where $r(i)$ is a random binary integer generated by K_3 and p is the pixel value of an original image with L bits per pixel.

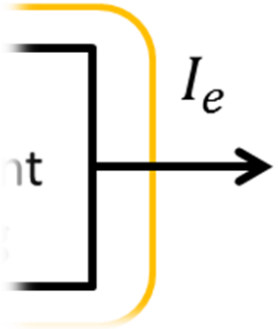
Step - 4



Step4: The three color components in each block are shuffled using a senary integer generated by the fourth secret key K_4.

Block scrambling-based steps

- L'immagine cifrata ottenuta I_e, risulta compatibile con lo standard JPEG
  - preservando la stessa efficienza di compressione dell'immagine JPEG originale



Cifratura immagine (16x16) blocchi

Original Image
$(X \times Y = 672\ x\ 480)$

Encrypted Image
$(B_x = B_y = 16,\ n = 1260)$

Schema proposto

Proposed scheme

- Nuovo schema di cifratura basato sulla cifratura ***Block-Scramling*** per il sistema ***EtC*** che evita alcuni effetti della ricompressione effettuata dai SNS provider
- Viene preservata la qualità dell'immagine ricompressa da un SNS provider
- Miglioramento della privacy

Encryption procedure

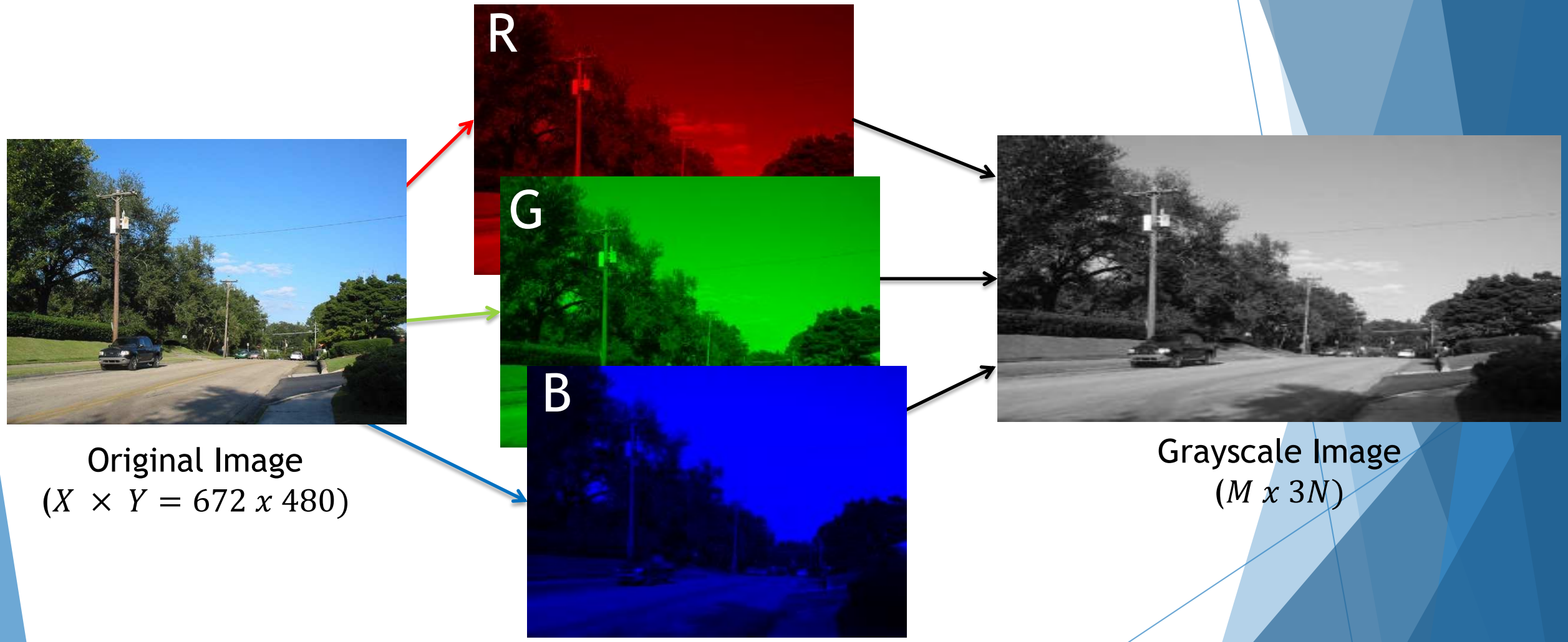
- Cifratura di un' immagine a colori di $M \times N$ pixel:

Step1: The RGB color components of the full-color image are separated into three individual channels. The scheme considers each channel as an individual image, and red, green, and blue channels can be respectively represented by i_r, i_g, and i_b.

Step2: i_r, i_g, and i_b are combined as a new image in grayscale (I_{gray}). For example, this combination process can be done vertically and horizontally, so size of the new image is equal to $M \times 3N$ or $3M \times N$.

Step3: Step 1 to step 3 of block scrambling-based encryption described in Section 2.1 is performed over I_{gray}.

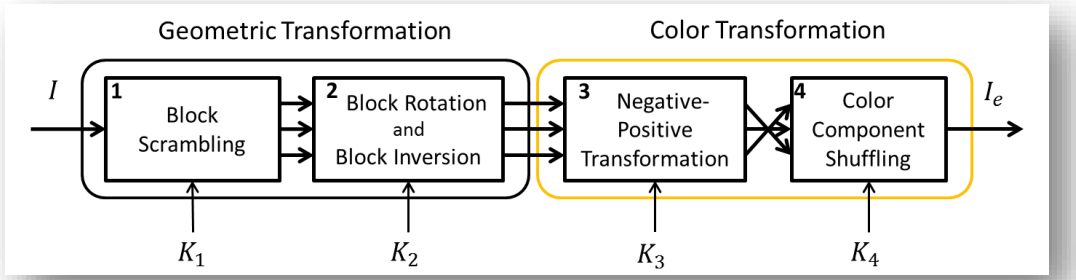
Encryption procedure - 1



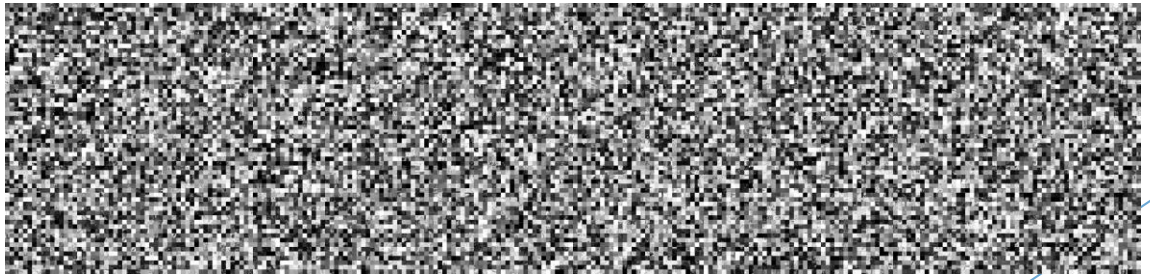
Original Image
$(X \times Y = 672\ x\ 480)$

Grayscale Image
$(M\ x\ 3N)$

Encryption procedure - 2

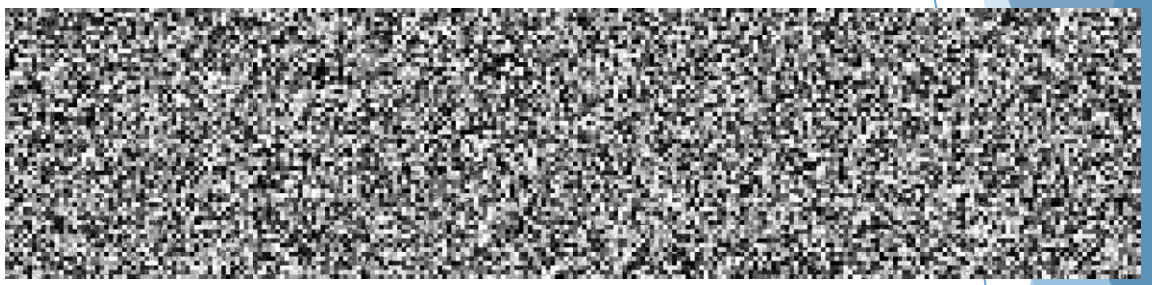


Encrypted Image
$(B_x = B_y = 8,\ n = 15120)$



Conventional scheme vs proposed scheme

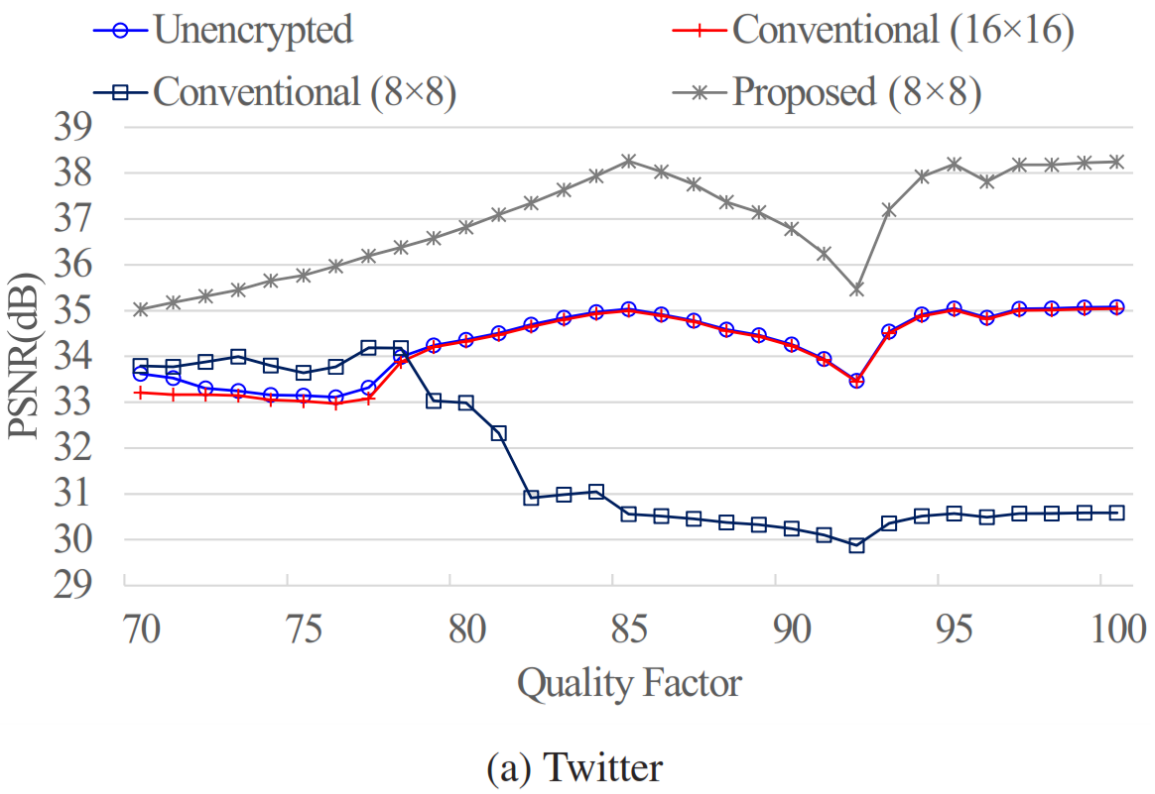
Encrypted Image
using conventional scheme
$(B_x = B_y = 16,\ n = 1260)$



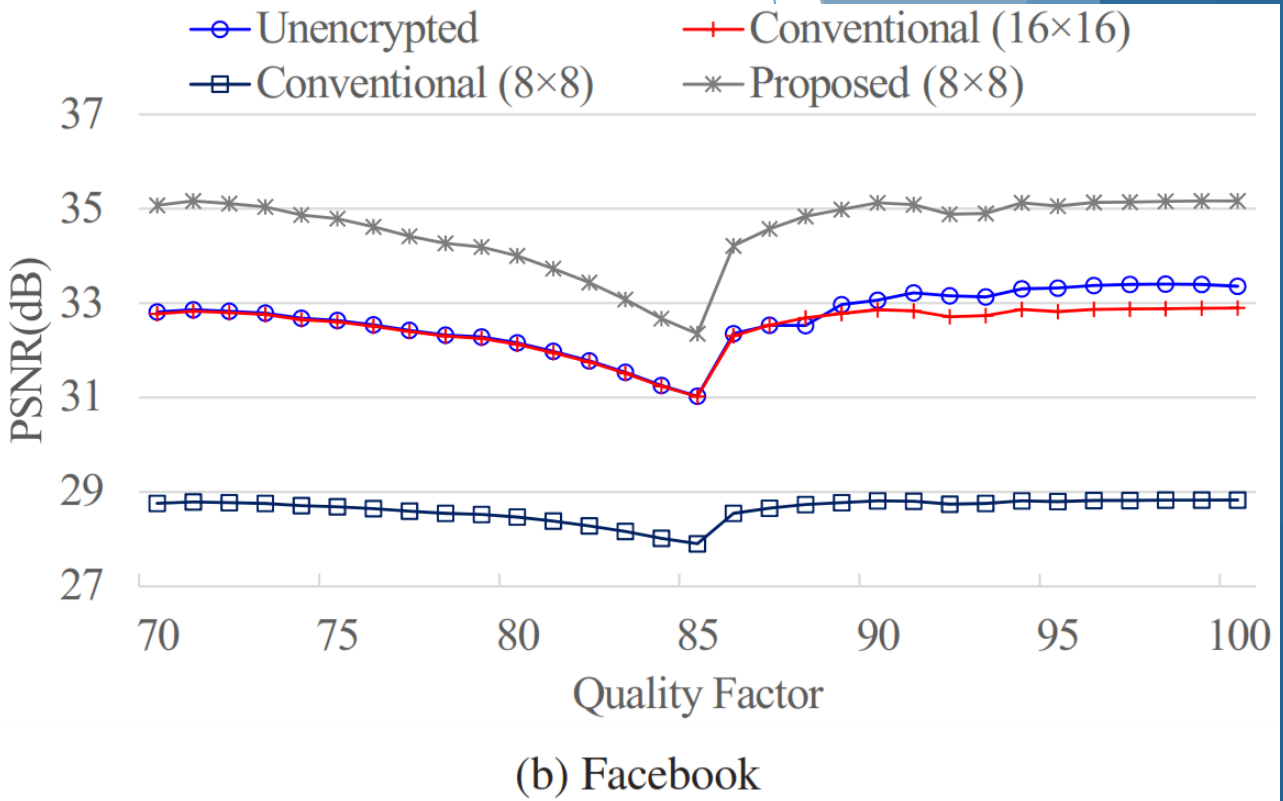
Encrypted Image
using proposed scheme
$(B_x = B_y = 8,\ n = 15120)$

- La dimensione di ogni blocco viene ridotta da (16x16) a (8x8)
- Il numero di blocchi totali, invece, è 12 volte più grande rispetto ad uno schema classico
- La dimensione dell'immagine cifrata è $3(M\ x\ N)$
- Migliora la ***privacy*** utilizzando meno informazioni sul colore

Risultati



(a) Twitter



(b) Facebook

- Lo schema proposto permette all'utente di scaricare un'immagine ad alta qualità

Conclusioni

- Implementazione dello schema
- Partire da una implementazione già esistente e migliorarla

GRAZIE PER L'ATTENZIONE